

明 細 書

通信システムおよび通信方法

技術分野

- [0001] 本発明は、認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信システムおよび通信方法に関する。

背景技術

- [0002] 従来、情報機器同士が通信を行う際、最も簡便な場合は、通信相手が如何なる機器であっても接続・通信を許可していた。また、複数の機器を対象に通信を行いたい場合、接続相手機器を識別してアクセス権を管理し、セキュリティを確保するために、ユーザIDとパスワードを用いて管理・運用する方法も広く用いられてきた。
- [0003] 特に、近年普及の著しいインターネットにおいては、ユーザIDとパスワードによるアクセス管理が広く一般に行われている。ユーザは、ネットワーク接続時にユーザIDとパスワード情報を送信し、認証されると通信を開始できるようになる。サーバ・クライアントモデルのネットワークでは、サーバ側にユーザIDとパスワードを記録・管理しておき、クライアントから接続要求が来た時に送られてくるユーザIDとパスワード情報を照合し、適合していればアクセス権を付与し、通信を開始するよう構成されている。ユーザが初めて通信を行う時は、予めユーザ情報をサーバ側に設定しておくか、ゲストアカウントで接続した後、ユーザID、パスワードをクライアント端末側から送信し、サーバ側に設定するよう構成されている。また、近年、ネットワークの物理媒体として電波を用いる無線ネットワークが普及してきている。無線ネットワークにおいても、サーバ・クライアントモデル・ネットワークは、上記と同様のアクセス権の管理が行われている。
- [0004] このようなアクセス権の管理機能が、Bluetoothに代表されるような近距離無線ネットワーク機器、特に携帯機器に実装される場合、使用される場所を選ばないので、今までに一度も接続したことのない機器同士が通信をする機会が増えることが予想される。また、無線通信なので、いつ、どの機器同士が接続しているのかがユーザには判り難く、通信していることに気付かない間にユーザの情報が盗まれる等の被害を防ぐためには、強固なセキュリティの実現が重要となる。Bluetooth規格では、上記セキ

セキュリティの問題に対応するため、機器間の接続通信前に認証を行う方法が考慮されている。Bluetooth規格におけるリンクレイヤーの機器認証の動作を以下に示す。

[0005] 図23は、Bluetooth規格での機器認証の動作を説明するための図である。機器認証は、1対1の機器間で行われるものであり、図23は、Bluetooth規格に基づく無線通信機能を搭載した2つの端末AとBとの間での認証処理時のやりとりと各端末内部で実行される処理について、時系列順に表したものである。図23の上部から下部へ向かって時間が経過するものとする。図23の左側の実線より左側が端末A内部を、右側の実線より右側が端末B内部を表している。また、図23の中央の2つの実線間の破線矢印が、端末Aと端末B間の電波による情報通信を示している。通信接続時に端末A、端末Bのどちらかが、通信相手を認証する認証側或いは被認証側として、認証プロセスを起動し、認証手続きの開始を要求する。ここでは、ユーザAが端末Aを、ユーザBが端末Bを操作するものとする。

[0006] 図23は、端末Aが通信相手を認証する認証側、端末Bが通信相手として認証される被認証側となる場合を示す。まず、端末AがステップS501で認証要求を端末Bへ送り、認証プロセスを起動する。端末BはステップS502で認証受付応答を返し、認証手続きを開始する。ステップS503では、端末A内部で生成した乱数1(531)を端末Bへ送信する一方、端末A自身の持つBluetoothパスキー(以下パスキー)と呼ばれる文字列または数字列を端末AのユーザAに入力させる。パスキーとは、Bluetooth対応端末が持つ機器固有のパスワード情報であり、今まで接続したことのない端末、言い換えると初めて接続する端末と認証手続きを行う際に使用される情報である。入力されたパスキーA(532)とパスキーAの長さであるパスキーA長533を演算アルゴリズム1A534の入力として使用する。演算アルゴリズム1A534は、初期化キー生成アルゴリズムであり、端末A内部で実行され、鍵情報である初期化キー1A538を生成する。乱数1(531)を受け取った端末B内部では、端末A同様、ユーザBに端末AのパスキーA535を入力させ、入力されたパスキーA535とパスキーAの長さであるパスキーA長536を演算アルゴリズム1B537の入力として使用する。なお、端末Aに対してユーザAが入力するパスキーA532と、端末Bに対してユーザBが入力するパスキーA535とは同一であるべきものである。換言すれば、認証側は、被認証側

が認証側のパスキーを正しく入力することを条件として、被認証側を認証側の通信相手として認証するのである。従って、パスキーA長533とパスキーA長536も同一となるべきものである。また、端末B内部で実行される演算アルゴリズム1B537と端末A内部で実行される演算アルゴリズム1A534も、同一のアルゴリズムである。端末Bでも端末Aと同様に初期化キー1B539が生成されるが、これも端末Aで生成される初期化キー1A538と同一となるべきものである。

[0007] 次に、端末Aは乱数1(531)とは異なる乱数2(540)を生成し、ステップS504において端末Bへ送信する。また、上記乱数2(540)、上記初期化キー1A538と被認証側である端末BのBluetooth Device Address(以下BD_ADDR_B)541を演算アルゴリズム2A542の入力として使用し、演算結果A545を得る。演算アルゴリズム2A542は、接続認証アルゴリズムであり、端末A内部で実行される。なお、BD_ADDR_Bは各Bluetooth機器固有のアドレス番号であり、かつ認証手続き処理を開始する前段階、すなわちステップS501を実行する前に、機器同士が接続を確立する際に交換する情報に含まれているので、この時点では既知の情報となっている。

[0008] 乱数2(540)を受け取った端末B内部では、端末A同様、乱数2(540)、上記初期化キー1B539と端末BのBD_ADDR_B543を演算アルゴリズム2B544の入力として使用し、演算結果B546を得る。端末B内部で実行される演算アルゴリズム2B544と端末A内部で実行される演算アルゴリズム2A542は、同一のアルゴリズムである。また、端末Aで使用するBD_ADDR_B541と、端末Bで使用するBD_ADDR_B543は、同一の情報である。

[0009] 次に、端末Bは、ステップS505において、演算結果B546を端末Aへ送信する。端末Aでは、ステップS505Aにおいて、端末A自身の内部で演算・生成した演算結果A545と、端末B内部で演算・生成されて端末Bから送信された演算結果B546とを比較する。演算結果Aと演算結果Bの値が等しければ、認証は成功とし、値が異なれば認証は失敗とする。認証が成功すると、端末Bを正当な通信相手として認証し、次の通信処理へと進む。また、認証に失敗した場合は、接続を切断して処理を終了する。

[0010] なお、セキュリティレベルをより高めるため、認証成功後、端末Aと端末Bの認証役

割を交換、すなわち、今度は端末Aが被認証側、端末Bが認証側となり、端末Bで生成する乱数と端末Bの持つパスキーBと端末AのBD_ADDR_Aをパラメータとして、図23と同様の手続きで認証を行い、端末相互で認証処理を行うことも可能である。ただし、上記役割を交換して行う認証処理は、省略可能である。

- [0011] 上述した認証動作は、通信を行う双方の端末共にユーザがパスキーを入力可能な場合である。しかし、Bluetoothを搭載した機器の中にはユーザがパスキーを直接入力することが困難であるか、又は直接入力できない機器も存在する。このような機器の場合、外部機器(メモリカード、ケーブルなど)から外部機器アクセス用インタフェースを介して、あらかじめパスキーを機器内蔵の不揮発性メモリに設定しておき、認証時には前記パスキーを内蔵不揮発性メモリなどから読み出して認証処理に使用することによって、パスキーの直接入力不能な機器のユーザがパスキーを入力しなくても良い方法が提案されている(例えば、特許文献1参照)。
- [0012] 図1は、従来の入力手段を持つBluetooth機器の内部構成を示すブロック図であり、図2は、従来の入力手段を持たないBluetooth機器のブロック図である。図1に示すBluetooth機器100は、外部機器を介してBluetooth機器100内のメモリに接続通信相手(Bluetooth機器2)のBD_ADDRとパスキーをあらかじめ書き込んでおき、認証処理時には上記BD_ADDRと上記パスキー読み出して使用するよう構成されている。図2に示すBluetooth機器200は、パスキーの入力手段を持たない機器であり、固定パスキーを本体内に記憶している。
- [0013] 図1に示すBluetooth機器100は、CPU101、ROM102、RAM103、不揮発性メモリ104、無線通信回路部105、アンテナ106、外部機器接続コネクタ107、インタフェース回路部108を有しており、図示するようにアンテナ106と外部機器接続コネクタ107を除く各構成要素は、内部バス113によって相互に接続されている。
- [0014] CPU101は、ROM102に格納されているプログラムに従って動作し、Bluetooth機器100の各種動作を制御する。ROM102は、Bluetooth機器100の制御手順、データ等をあらかじめ格納した不揮発性メモリである。RAM103は、外部機器から送信されるデータへの変換作業用のワークエリア、CPU101の演算等に使用するワークエリア、無線通信回路部から送受信される通信データ、各種設定等を一時的に格

納するエリアとして使用される。不揮発性メモリ104は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD__ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。無線通信回路部105は、無線通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD__ADDR__D、自身のパスキーDを記憶している不揮発性メモリ等から構成され、アンテナ106が接続されている。

- [0015] 外部機器接続コネクタ107は、外部機器とBluetooth機器100を接続するためのインタフェースであり、例えば、メモリカード、コネクタなどが想定される。外部機器接続用インタフェース回路部108は、外部機器との間でデータ通信を行う機能を備えている。CPU101の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。
- [0016] 図2に示すBluetooth機器200は、CPU201、ROM202、RAM203、不揮発性メモリ204、無線通信回路部205、アンテナ206を有しており、図示するように内部バス212によって相互に接続されている。
- [0017] CPU201は、ROM202に格納されているプログラムに従って動作し、Bluetooth機器200の各種動作を制御する。ROM202はBluetooth機器200の制御手順、データ等を予め格納した不揮発性メモリである。RAM203は外部機器から送信されるデータへの変換作業用のワークエリア、CPU101の演算等に使用するワークエリア、無線通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。
- [0018] 不揮発性メモリ204は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD__ADDR、以前接続した他のBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。
- [0019] 無線通信回路部205は、無線通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD__ADDR__P、自身のパスキーPを記憶している不揮発性メモリ等から構成され、アンテナ206が接続されている。
- [0020] 従来、Bluetooth機器100には、パスキー入力機能の無いBluetooth機器200との間で認証処理を行うために、以下の設定が行われる。図1に示すBluetooth機器

100の外部機器接続インタフェースにメモ리카ードまたは、ケーブルを接続し、あらかじめ調べておいたBluetooth機器200のBluetoothアドレス(BD__ADDR__P)とBluetooth機器200のパスキー情報(パスキーP)をリスト情報として、Bluetooth機器100における不揮発性メモリ204の所定のエリアに書き込んでおく。

[0021] 図3は、従来のBluetoothアドレスとパスキーのリストを示す図であり、不揮発性メモリ204内に格納されているパスキーリスト1301の例を示す。同図に示すように、BD__ADDRとパスキーとはペアとして格納されている。図3では(BD__ADDR__P1202、パスキーP1203)、(BD__ADDR__R1204、パスキーR1205)の2つのペアを持っている。ここでは2つのペアのパスキーリストを例示したが、ペアの個数に特に制限はない。

[0022] 図4は、従来のBluetoothの接続認証シーケンスを示す図であり、Bluetooth機器200が認証側、Bluetooth機器100が被認証側として認証手続きを行う場合の認証処理を示す。まず、Bluetooth機器200がBluetooth機器100に対して認証手続きを要求する(ステップS801)。Bluetooth機器200からの認証要求を受け取ったBluetooth機器100は、パスキー検索処理831を実行する。パスキー検索処理831の結果、Bluetooth機器200のBD__ADDR__PおよびパスキーPが存在する場合は認証要求受付応答を、存在しない場合は被認証側としての認証要求は受け付けずBluetooth機器200に対して認証側と被認証側との役割を交換し、Bluetooth機器100が認証側となることを要求する認証役割交換要求を応答として送信する(ステップS802)。

[0023] 図5は、従来のBluetoothの接続認証フローを示す図であり、図4に示したパスキー検索処理831の詳細を示す。なお、図5は、処理内容を一般化して示しているが、ここでは、今までの説明で用いた例に沿って説明する。まず、認証要求を送信してきたBluetooth機器200が今回初めて接続する相手かどうかを判断する(ステップS901)。具体的には、Bluetooth機器100の不揮発性メモリ104中に記憶されている機器接続リストの中に、Bluetooth機器200のBD__ADDR__Pに合致するBD__ADDRと、接続に必要なリンクキーPがリストアップされているかどうかを検索する。リストアップされていなければ、初めて接続する機器であるのでステップS902へ進み、リス

トアップされていれば、ステップS904へ進む。

[0024] 図6は、従来のBluetooth機器におけるBluetoothアドレスとリンクキーのリストを示す図であり、機器接続リストの例を示す。BD__ADDRと前回認証接続時に生成したLINK KEYをペアとしたリスト1101として格納されている。図6には、(BD__ADDR__A1102、KEY__A1103)、(BD__ADDR__F1104、KEY__F1105)、(BD__ADDR__Z1106、KEY__Z1107)の3つのペアが記憶されており、ステップS901において、この機器接続リスト1101の中からBluetooth機器200のBD__ADDRであるBD__ADDR__Pを検索し、有るか否かを判定する。図6の機器接続リスト1101には、BD__ADDR__Pが登録されていないので、Bluetooth機器200は初めて接続する機器と判断され、ステップS902へ進むことになる。

[0025] 次に、Bluetooth機器100に格納されたパスキーリスト1301の中に、Bluetooth機器200のBD__ADDR__PとパスキーPがリストアップされているかどうかを検索する(ステップS902)。そして、Bluetooth機器200のBD__ADDR__P1302に対応するパスキーP1304がリストアップされているか否かを判定する(ステップS903)。パスキーP1304が存在すればステップS904へ進み、存在しなければステップS905へ進む。

[0026] ステップS904では、Bluetooth機器200へ返す応答として、認証要求受け入れを選択する。ステップS905では、パスキー検索処理831を起動する要因が、認証要求か否かを判定する。その結果、認証要求であった場合はステップS906へ進み、認証役割交換要求であった場合はステップS907へ進む。

[0027] ステップS906では、Bluetooth機器200へ返す応答として認証役割交換要求を選択し、ステップS907では、Bluetooth機器200へ返す応答として認証要求拒否を選択する。ステップS904、906、907の何れかの処理を行った後、パスキー検索処理831を終了する。

[0028] 図7は、従来のBluetoothの接続認証シーケンスを示す図であり、図4とは逆に、Bluetooth機器200が被認証側、Bluetooth機器100が認証側となって認証手続きを行う場合の認証処理を示す。ここでは、図4のように、Bluetooth機器200がBluetooth機器100に対して認証手続きを要求するのではなく、Bluetooth機器100が認

証側となってBluetooth機器200に対して認証手続きを要求する(ステップS1001)。Bluetooth機器100からの認証要求を受け取ったBluetooth機器200は、パスキー入力手段を持たないため、認証要求を拒否し、Bluetooth機器100に対して認証役割交換要求を送信する(ステップS1002)。Bluetooth機器200からの認証役割交換要求を受け取ったBluetooth機器100は、パスキー検索処理1031を実行する。ここで行うパスキー検索処理1031は、図4、図5に示したパスキー検索処理831と同じである。パスキー検索処理1031の結果、Bluetooth機器200のBD_ADDR_P、パスキーPが存在する場合は認証要求受付応答を、存在しない場合は被認証側としての認証要求は受け付けず、Bluetooth機器200に認証要求拒否応答を送信する(ステップS1003)。

[0029] 上述したように、従来の技術によれば、ユーザがパスキーを入力できないか、或いはパスキーの入力が困難な端末同士が通信開始時に認証処理を行う場合には、どちらか一方の端末が、外部機器によって予め本体内のメモリに設定された通信相手端末のBD_ADDRとパスキーのBD_ADDR_PとパスキーPを読み出して使用することにより、認証処理を行うことができた。

[0030] しかし、従来のBluetooth認証方法及び通信システムにおいては、外部機器を介して予め通信相手端末の認証情報BD_ADDRとパスキーを取得し、本体内のメモリに上記認証情報を設定するために外部機器アクセス用の外部機器接続コネクタ107とインタフェース回路部108を装備する必要がある。すなわち、従来は、本来製品によっては必ずしも必要の無い上記外部機器アクセス用インタフェース回路部を設ける必要があり、ユーザにとっては使い難く、メーカーにとっては製品コストを高くする要因となっていた。

[0031] 図8は、従来のBluetooth機器同士のネットワーク形態の1例を示す図である。同図において、Bluetooth機器同士が互いにBluetooth接続するものとする。例えば、Bluetooth機器2001は、隣接するBluetooth機器2002、及びBluetooth機器2008とBluetooth接続する。Bluetooth接続には、前述したように接続先Bluetooth機器の持つパスキー情報が必要である。よって、図8においてはBluetooth機器2001は、隣接するBluetooth機器2001とBluetooth機器2008のパスキー情報を外部

機器から取得する必要がある。これは、他のBluetooth機器2002～2008においても同様である。

[0032] 従って、従来の技術では、図8のようなBluetoothネットワークの形態において、各Bluetooth機器に上記外部機器接続用コネクタ及びインタフェース回路が必要となり、Bluetoothを搭載した製品のコストが高くなる要因になっている。

[0033] また、工場出荷時にBluetooth機器の内蔵不揮発性メモリにあらかじめ、接続先相手のBluetooth機器の認証情報を記憶しておく方法もあるが、この方法では上記工場出荷時に記憶した特定のBluetooth機器だけしかBluetooth接続できない。他のBluetooth機器製品と接続させる場合には、Bluetooth機器の内蔵不揮発性メモリの認証情報を変更するしかなく、外部インタフェースを持たないBluetooth機器の場合は、他の任意のBluetooth機器とのBluetooth接続は不可能である。このため、Bluetoothの相互接続も低くなり、ユーザにとって扱いにくい場合がある。

[0034] 特許文献1:特開2003-152713号公報

発明の開示

発明が解決しようとする課題

[0035] 上述したように、従来の通信システムおよび通信方法においては、認証情報を入力するために各通信機器に外部機器アクセス用インタフェースを新たに設ける必要があり、通信システムとしてのコストが高くなってしまふ。

[0036] 本発明は、このような事情に鑑みてなされたものであり、認証情報を入力するための外部機器アクセス用インタフェースを新たに設けることなく通信機器に認証情報を入力できる通信システムおよび通信方法を提供することを目的としている。

課題を解決するための手段

[0037] 本発明の通信システムは、認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信システムであって、前記少なくとも2台のうち少なくとも1台の通信機器に対して、無線を介して前記認証情報を供給する通信部を備える。

[0038] 上記構成によれば、通信機器に対して、無線を介して前記認証情報を供給することにより、通信機器は、従来の無線通信機能を利用して認証情報を取得でき新たに

認証情報の入力手段を設ける必要がない為、通信システムのコストを削減できる。

- [0039] また、本発明の通信システムは、前記通信部が、前記少なくとも2台の通信機器のうち特定の通信機器に備えられていることを特徴とする。また、本発明の通信システムは、前記特定の通信機器に備えられた前記通信部が、前記少なくとも2台の通信機器のうち前記特定の通信機器以外の通信機器に対して、前記認証情報を供給することを特徴とする。また、本発明の通信システムは、前記通信部が、前記少なくとも2台の通信機器と独立に備えられていることを特徴とする。
- [0040] また、本発明の通信システムは、前記通信部が、外部インタフェースを備え、前記外部インタフェース経由で前記認証情報を受け取ることを特徴とする。
- [0041] また、本発明の通信システムは、前記外部インタフェースに接続されたメモリカードに保存された前記認証情報を前記外部インタフェース経由で受け取ることを特徴とする。上記構成によれば、メモリカード上で暗号化された情報を認証情報として利用することが可能となり、通信システムの安全性を高めることができる。
- [0042] また、本発明の通信システムは、前記少なくとも1台の通信機器が、各通信機器に予め定められた固有の第1の認証情報を用いて前記通信部と認証を行う機能と、前記第1の認証情報とは異なる第2の認証情報を用いて前記少なくとも2台の通信機器間の認証を行う機能とを備えることを特徴とする。上記構成によれば、通信機器と通信部とが第1の認証情報を用いて認証を行った後に、通信部が通信機器に第2の認証情報を送ることにより、通信システムの安全性を高めることができる。
- [0043] また、本発明の通信システムは、前記認証情報が、予め各通信機器に定められ前記通信部と前記少なくとも1台の通信機器との間で用いられる各機器固有の固定認証情報と、任意に生成され前記少なくとも2台の通信機器間の通信に用いられる可変認証情報とを含むことを特徴とする。また、本発明の通信システムは、前記認証情報が、通信相手のアドレス情報またはパスワード情報であることを特徴とする。
- [0044] 上記構成によれば、通信機器間で使用される認証情報と、通信部と通信機器との間で使用される認証情報とが異なることにより、通信システムの安全性を高めることができる。
- [0045] また、本発明の通信システムは、前記少なくとも2台の通信機器間の通信または前

記少なくとも1台の通信機器と前記通信部との間の通信が、Bluetooth規格の無線通信であることを特徴とする。

[0046] また、本発明の通信方法は、認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信方法であって、前記少なくとも2台の通信機器のうち少なくとも1台の通信機器に対して、無線を介して前記認証情報を供給する供給ステップを有する。

[0047] また、本発明の通信方法は、前記供給ステップが、前記少なくとも2台の通信機器のうち特定の通信機器と前記少なくとも2台の通信機器のうち前記特定の通信機器以外の通信機器間で実行されることを特徴とする。また、本発明の通信方法は、前記少なくとも1台の通信機器に対して、前記少なくとも1台の通信機器に予め定められた固有の第1の認証情報を用いて認証を行なう第1の認証ステップをさらに有し、前記第1の認証ステップで認証された場合に、前記認証情報は前記少なくとも1台の通信機器に供給されることを特徴とする。また、本発明の通信方法は、前記少なくとも1台の通信機器が受け取る前記第1の認証情報とは異なる第2の認証情報を用いて前記少なくとも2台の通信機器間の認証を行なう第2の認証ステップをさらに有する。また、本発明の通信方法は、前記少なくとも2台の通信機器間の通信または前記少なくとも1台の通信機器への通信が、Bluetooth規格の無線通信であることを特徴とする。

[0048] また、本発明の通信機器は、認証情報を用いて互いに通信可能であるか認証する機能を有し認証後に通信を開始する通信機器であって、前記認証情報を無線を介して取得する手段を備える。上記構成によれば、従来の無線通信機能を利用して認証情報を取得でき新たに認証情報の入力手段を設ける必要がない為、通信機器のコストを削減できる。

発明の効果

[0049] 本発明の通信システムおよび通信方法によれば、通信機器に対して、無線を介して前記認証情報を供給することにより、通信機器は、従来の無線通信機能を利用して認証情報を取得でき新たに認証情報の入力手段を設ける必要がない為、通信システムのコストを削減できる。

図面の簡単な説明

- [0050] [図1]従来の入力手段を持つBluetooth機器の内部構成を示すブロック図
- [図2]従来の入力手段を持たないBluetooth機器の内部構成を示すブロック図
- [図3]従来のBluetoothアドレスとパスキーのリストを示す図
- [図4]従来のBluetoothの接続認証シーケンスを示す図
- [図5]従来のBluetoothの接続認証フローを示す図
- [図6]従来のBluetooth機器におけるBluetoothアドレスとリンクキーのリストを示す図
- [図7]従来のBluetoothの接続認証シーケンスを示す図
- [図8]従来のBluetooth機器同士のネットワーク形態の1例を示す図
- [図9]本発明の第1の実施形態を説明するためのBluetooth機器通信システムの構成図
- [図10]第1の実施形態のBluetoothセキュリティサーバの内部構成を示す図
- [図11]第1の実施形態のBluetooth機器の内部構成を示す図
- [図12]第1の実施形態のBluetoothセキュリティサーバの認証情報配布フローを示す図
- [図13]第1の実施形態のクラスデバイスとパスキーのリストの例を示す図
- [図14]第1の実施形態のBluetooth機器の認証情報配布フローを示す図
- [図15]第1の実施形態のBluetooth機器同士のネットワーク形態の例を示す図
- [図16]本発明の第2の実施形態のBluetoothセキュリティサーバの内部構成図
- [図17]第2の実施形態のBluetoothセキュリティサーバ認証情報配布フローを示す図
- [図18]本発明の第3の実施形態のBluetoothセキュリティサーバの認証情報配布フローを示す図
- [図19]第3の実施形態のBluetooth機器におけるBluetoothアドレスとリンクキーのリストを示す図
- [図20]第3の実施形態のBluetooth機器の認証情報配布フローを示す図
- [図21]本発明の第4の実施形態のBluetoothセキュリティサーバの認証設定時動作フローを示す図

[図22]第4の実施形態におけるBluetooth機器の認証設定の動作フローを示す図

[図23]Bluetooth規格での機器認証の動作を説明するための図

符号の説明

[0051] 404 操作部

405、604、1204 不揮発性メモリ

406、605、1205 無線通信回路部

703 入力認証情報

702a、702b 認証情報

703 Bluetoothセキュリティサーバ

704、705 Bluetooth機器

1207 外部機器接続コネクタ

1208 インタフェース回路部

1209 メモリカード

発明を実施するための最良の形態

[0052] (第1の実施形態)

図9は、本発明の第1の実施形態を説明するためのBluetooth機器通信システムの構成図であり、Bluetooth認証情報配布の概念を示す。同図に示す通信システムは、認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能なBluetooth通信システムであって、Bluetooth機器1(704)およびBluetooth機器2(705)と、Bluetooth機器1(704)およびBluetooth機器2(705)に対して、無線を介して認証情報を供給するセキュリティサーバ703を備える。

[0053] Bluetoothセキュリティサーバ703は、Bluetooth機器1(704)およびBluetooth機器2(705)と認証接続し、無線を介して認証情報(接続通信相手のBD_ADDRとパスキー、またはパスキーのみ)702(702a、702b)を配布するように構成されている。ここで、認証情報702は、Bluetooth機器が他のBluetooth機器と通信するためのものであり、Bluetooth機器703とBluetooth機器704がBluetooth認証接続する場合に用いる認証情報である。本実施形態ではBluetoothセキュリティサーバ703は、Bluetooth機器と独立に備えられているが、Bluetooth機器に対して無線を介

して認証情報を供給する機能が、いずれかのBluetooth機器に備えられていてもよい。

- [0054] また、Bluetooth機器1(704)およびBluetooth機器2(705)は、各通信機器に予め定められた固有の既存認証情報(第1の認証情報)を用いてBluetoothセキュリティサーバ703と認証を行う機能と、既存認証情報とは異なる認証情報(第2の認証情報)を用いてBluetooth機器1(704)、2(705)間の認証を行う機能とを備える。Bluetooth機器1(704)およびBluetooth機器2(705)は、Bluetoothセキュリティサーバ703からの認証情報702a、702bが配布される前に、各機器に固有となる予め定められた既存認証情報(第1の認証情報)が設定されているものとする。Bluetoothセキュリティサーバ703は、Bluetooth機器1(704)およびBluetooth機器2(705)の既存認証情報をあらかじめ既知のものとする。既存認証情報は外部者には漏れていない情報とする。Bluetooth機器1(704)およびBluetooth機器2(705)は、認証情報の入力手段を持たず、Bluetoothセキュリティサーバ703は、認証情報の入力手段を持つ機器である。
- [0055] Bluetooth機器1(704)およびBluetooth機器2(705)は、既存認証情報と異なる認証情報702(第2の認証情報)をBluetoothセキュリティサーバ703から無線を介して取得し、不揮発性メモリに記憶する。Bluetooth機器704とBluetooth機器705がBluetooth認証接続する場合、上記不揮発性メモリから認証情報を読み出し、認証処理時に使用する。
- [0056] 図10は、第1の実施形態のBluetoothセキュリティサーバ703の内部構成を示す図である。Bluetoothセキュリティサーバ703は、通信機器に対して、無線を介して認証情報を供給するものであり、CPU401、ROM402、RAM403、操作部404、不揮発性メモリ405、無線通信回路部406、アンテナ407を有している。図示するように、アンテナ407を除く各構成要素は、内部バス413によって相互に接続されている。CPU401は、ROM402に格納されているプログラムに従って動作し、Bluetoothセキュリティサーバ703の各種動作を制御する。ROM402はBluetoothセキュリティサーバ703の制御手順、データ等をあらかじめ格納した不揮発性メモリである。RAM403は外部機器から送信されるデータへの変換作業用のワークエリア、CPU401

の演算等に使用するワークエリア、無線通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。操作部404は、外部からの入力装置であり、ボタンやタッチパネルなどで構成される。Bluetoothセキュリティサーバの使用者は、操作部404を用いてデバイス検索、認証情報の入力などを行なう。

[0057] 不揮発性メモリ405は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。無線通信回路部406は、無線通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD_ADDR_D、自身のパスキーDを記憶している不揮発性メモリ等から構成され、アンテナ407が接続されている。

[0058] 図11は、第1の実施形態のBluetooth機器600の内部構成を示す図である。同図に示すように、Bluetooth機器600は、CPU601、ROM602、RAM603、不揮発性メモリ604、無線通信回路部605、アンテナ606を有し、他の通信機器と通信可能であるか認証した後に通信を開始する通信機器である。図示するように、アンテナ606を除く各構成要素は内部バス613によって相互に接続されている。CPU601は、ROM602に格納されているプログラムに従って動作し、Bluetooth機器600の各種動作を制御する。ROM602はBluetooth機器600の制御手順、データ等をあらかじめ格納した不揮発性メモリである。RAM603は外部機器から送信されるデータへの変換作業用のワークエリア、CPU601の演算等に使用するワークエリア、無線通信回路部605から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。不揮発性メモリ604は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。無線通信回路部605は、無線通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD_ADDR_D、自身のパスキーDを記憶している不揮発性メモリ等から構成され、アンテナ606が接続されている。また、無線通信回路部605は、アンテナ606が受信した情報から認証情報を抽出して取得する機能を有する。アンテナ

ナ606及び無線通信回路部605は、他の通信機器と通信するための認証情報を無線を介して取得し、CPU601は、取得した認証情報を用いて認証を行う。

[0059] 次に、図9に示した認証情報702(第2の認証情報)の配布の詳細を図11、12、13に基づいて説明する。

[0060] 図12は、第1の実施形態のBluetoothセキュリティサーバ703の認証情報配布フローを示す図である。最初に、Bluetoothセキュリティサーバ703が、デバイス検索のためにインクワイアリ検索を使用する(ステップS601)。また、応答してきたBluetooth機器のBD_ADDRとそのデバイスクラスが所望のBluetooth機器1(704)またはBluetooth機器2(705)のものであるか確認する。Bluetooth機器1(704)またはBluetooth機器2(705)であった場合、ステップS602へ進み、そうでなければ終了する。次に、ステップS602では、メーカーから購入後初めての使用の場合であるときは、ステップS603へ進み、そうでない場合は、ステップS604へ進む。ステップS603では、Bluetoothセキュリティサーバ側は、ROM402に保存している既存認証情報(第1の認証情報)を認証に使用する。ここで、既存認証情報は工場出荷時にメーカーが機種固有に設定した値であり、外部者には漏れていないものとする。工場出荷時には、Bluetooth機器は機種固有の既存認証情報を事前に不揮発性メモリ604に書き込まれているものとする。その後、製品購入時にBluetoothセキュリティサーバを使用して、既存認証情報をユーザ独自に変更する。この場合、Bluetoothセキュリティサーバ703内部にも工場出荷時の機種固有の既存認証情報があらかじめ設定されており、Bluetoothセキュリティサーバ使用者には既存認証情報の値は表示されないものとする。

[0061] 図13は、第1の実施形態のクラスデバイスとパスキーのリストの例を示す図である。図13では、各デバイスクラス毎に初期接続パスキーが設定されており、Bluetoothセキュリティサーバ703側は、該パスキーを認証時に使用する。Bluetooth機器1(704)またはBluetooth機器2(705)側では、不揮発性メモリ604に同様の既存認証情報が工場出荷時に設定されている。ステップS604では、操作部404を用いてBluetooth機器1(704)またはBluetooth機器2(705)の既存認証情報をユーザに入力してもらう。ステップS605では、認証結果がOKならばステップS607に進み、認証を

受諾してステップS608に進む。そうでない場合は、ステップS606に進み認証を拒否して終了する。

[0062] ステップS608では、Bluetoothセキュリティサーバ703とBluetooth機器1(704)またはBluetooth機器2(705)がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。確認がOKの場合は、ステップS609に進み、BluetoothセキュリティサーバからBluetooth機器1(704)またはBluetooth機器2(705)に認証情報(第2の認証情報)を配布する。この際、Bluetoothセキュリティサーバ703は、操作部404を用いてBluetoothセキュリティサーバ使用者に入力された認証情報をBluetooth機器1(704)またはBluetooth機器2(705)に配布する。Bluetooth機器1(704)またはBluetooth機器2(705)はそれまでの既存認証情報(第1の認証情報)を破棄し、配布された新しい認証情報(第2の認証情報)を保存する。以上をもって認証の配布処理を終了する。

[0063] 図14は、Bluetooth機器の認証情報配布フローを示す図であり、Bluetooth機器1(704)を例に、Bluetooth機器側の動作を説明する。最初に、Bluetoothセキュリティサーバ703からBluetooth機器704に対して認証接続を開始する。ステップS2401において不揮発性メモリ604から既存認証情報(第1の認証情報)を取得し、Bluetoothセキュリティサーバ703との認証に使用する。ステップ2402では、認証結果がOKならばステップS2403に進み、認証受諾してステップS2404に進む。そうでない場合は、ステップS2407に進む認証を拒否して終了する。ステップS2404では、Bluetoothセキュリティサーバ703とBluetooth機器704がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。確認がOKの場合は、ステップS2405に進み、Bluetoothセキュリティサーバ703からBluetooth機器704に認証情報(第2の認証情報)を配布する。そうでない場合は、終了する。次にステップS2406に進み、該不揮発性メモリに取得した該認証情報を記憶し終了する。また、以上の動作は、Bluetooth機器2(705)においても同様に行われる。

[0064] 図23は、Bluetooth規格での機器認証の動作を説明するための図であり、Bluetooth機器1(704)とBluetooth機器2(705)との認証処理を示す。Bluetooth機器間での認証処理は従来と同様なので説明を省略する。

- [0065] 従来技術においては、Bluetooth機器の外部インタフェースを介して外部機器からBD_ADDRとパスキーをBluetooth機器内の不揮発性メモリに書き込んだが、第1の実施形態においては、Bluetooth機器に装備した無線を介してBluetooth機器内の不揮発性メモリに書きこむ点が異なる。ここで、外部インタフェース及び外部インタフェースを介して接続される外部機器として、USBケーブルなどで接続されるUSBデバイスや、直接にスロットに挿入されるメモリカードなどが用いられることが想定される。また、図11のように第1の実施形態のBluetooth機器の構成は、従来の構成を示す図1のように外部接続用のインタフェース回路部108と外部接続機器コネクタ107を必要としないため、製品コストを低く抑えることが可能となる。
- [0066] ここで、補足として第1の実施形態を、図8に示す従来のBluetoothネットワーク形態に応用した例を説明する。
- [0067] 図15は、第1の実施形態のBluetooth機器同士のネットワーク形態の例を示す図である。同図において、図8と同様にBluetooth機器同士が互いにBluetooth接続するものとする。例えば、Bluetooth機器3001は、隣接するBluetooth機器3002及びBluetooth機器3008とBluetooth接続される。Bluetooth接続するためには、前述したように接続先Bluetooth機器の持つパスキー情報が必要である。よって、図15においてはBluetooth機器3001は、隣接するBluetooth機器3001とBluetooth機器3008のパスキー情報を取得する必要がある。本実施形態においては、Bluetoothセキュリティサーバ3009から、各Bluetooth機器3001〜3008に前記手法により無線を介して認証情報を配布する。
- [0068] 従って、本実施形態においては、図15に示す、従来と同様のネットワーク形態であっても、外部機器接続用コネクタ及びインタフェース回路を各Bluetooth機器3001〜3008に設ける必要はない。また、外部インタフェースを持たないBluetooth機器であっても、任意の他Bluetooth機器とのBluetooth接続が可能であるため、Bluetoothの相互接続も維持され、ユーザにとっては使い易い製品となっている。また、Bluetoothセキュリティサーバ703は単独の機器としているが、Bluetoothネットワークを構成する機器のうちどれか1台のBluetooth機器の内蔵機能として追加しても良い。

[0069] (第2の実施形態)

第1の実施形態では、Bluetoothセキュリティサーバの使用者が認証情報を直接入力した。また、第1の実施形態では、該認証情報が変更された場合または該認証情報を第3者から完全に隠蔽したい場合等に、改良の余地がある。そこで、第2の実施形態では、Bluetoothセキュリティサーバに外部インタフェースを具備し、該外部インタフェースからBluetooth機器への配布用認証情報を入力する。

[0070] 図16は、本発明の第2の実施形態のBluetoothセキュリティサーバの内部構成図である。同図に示すように、Bluetoothセキュリティサーバ1209は、メモ리카ードを装着するための外部機器接続コネクタ1207を備える。Bluetoothセキュリティサーバ1200に装着可能なメモ리카ード1209は、パーソナルコンピュータ等の外部機器のメモ리카ードスロットへ装着され、あらかじめ調査したBluetooth機器のBD_ADDRとパスキー情報とが、メモ리카ードの所定のエリアに書き込まれている。通信を行う場合は、メモ리카ード1209を外部機器接続コネクタ1207に装着しておく。なお、メモ리카ード1209内に設定されているBD_ADDRとパスキーリストは、第1の実施形態で説明したBluetoothセキュリティサーバ703内蔵の不揮発性メモリ404内のリストと同様のものである。第1の実施形態では、操作部404を用いて、Bluetoothセキュリティサーバ703に認証情報を入力していたが、第2の実施形態では、Bluetoothセキュリティサーバ1200に具備した外部インタフェースを用いて認証情報を入力する点が異なる。

[0071] 図16に示すように、Bluetoothセキュリティサーバ1200は、CPU1201、ROM1202、RAM1203、不揮発性メモリ1204、無線通信回路部1205、アンテナ1206、外部機器接続コネクタ1207、インタフェース回路部1208を有しており、図示するように、内部バス1213によって相互に接続されている。CPU1201は、ROM1202に格納されているプログラムに従って動作し、Bluetoothセキュリティサーバ1200の各種動作を制御する。ROM1202はBluetoothセキュリティサーバ1200の制御手順、データ等をあらかじめ格納した不揮発性メモリである。RAM1203は外部機器から送信されるデータへの変換作業用のワークエリア、CPU1201の演算等に使用するワークエリア、無線通信回路部1205から送受信される通信データ、各種設定等を一時的

に格納するエリアとして使用される。不揮発性メモリ1204は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手のBD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。無線通信回路部1205は、無線通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD_ADDR_D、自身のパスキーDを記憶している不揮発性メモリ等から構成され、アンテナ1206が接続されている。外部機器接続コネクタ1207は、外部機器とBluetoothセキュリティサーバを接続するコネクタである。インタフェース回路部1208は、外部機器接続コネクタ1207を介して接続された外部機器との間でデータ通信を行う機能を備えている。CPU1201の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

[0072] 図17は、第2の実施形態のBluetoothセキュリティサーバ認証情報配布フローを示す図であり、Bluetoothセキュリティサーバ1200からBluetooth機器への認証情報の配布の詳細を示す。まず、Bluetoothセキュリティサーバ1200が、デバイス検索のためにインクワイアリ検索を使用する(ステップS2301)。応答してきたBluetooth機器のBD_ADDRとそのデバイスクラスが所望のBluetooth機器のものであるか確認する。所望のBluetooth機器であった場合、ステップS2302へ進み、そうでなければ終了する。

[0073] 次に、ステップS2302では、Bluetoothセキュリティサーバにメモリカードが挿入されていた場合は、ステップS2303へ進み、そうでない場合は、ステップS2304へ進む。ステップS2303では、Bluetoothセキュリティサーバ側は、Bluetooth機器の既存認証情報が保存されたメモリカードを使用する。S2304では、不揮発性メモリ1204に保存している既存認証情報を認証に使用する。ここで、不揮発性メモリ1204に保存されている既存認証情報は、工場出荷時にメーカーが機種固有に設定した値であり、外部者には漏れていないものとする。工場出荷時には、Bluetooth機器は機種固有の既存認証情報を事前に不揮発性メモリに書き込まれているものとする。Bluetooth機器の工場出荷時の認証情報が変更された場合は、変更された既存認証情報を記憶したメモリカードをBluetoothセキュリティサーバに挿入し、S2303の処理を行なう。ここで、該メモリカードはメーカーから配布されるもので、一般ユーザには参照

不可なメモリカードとするべきである。第1の実施形態と同様に、第2の実施形態においても、製品購入時に、Bluetoothセキュリティサーバを使用して、Bluetooth機器の上記認証情報をユーザ独自に変更する。

[0074] ステップS2305では、認証結果がOKならばステップS2307に進み、認証を受諾してステップS2308に進む。そうでない場合は、ステップS2306に進み認証を拒否して終了する。ステップS2308では、BluetoothセキュリティサーバとBluetooth機器がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。確認がOKの場合は、ステップS2309に進み、BluetoothセキュリティサーバからBluetooth機器に認証情報を配布する。Bluetooth機器は前回の認証情報を破棄し、配布された新しい認証情報を保存する。以上で認証情報の配布処理を終了する。

[0075] 第2の実施形態におけるBluetooth機器側の動作は、第1の実施形態と同様なので説明を省略する。

[0076] 第2の実施形態によれば、メモリカードを装着して認証情報をBluetoothセキュリティサーバに入力するため、外部者に漏れることなく安全に認証情報を入力することができる。また、Bluetoothセキュリティサーバとメモリカード1209間、または上記パーソナルコンピュータとメモリカード1209間でセキュワを保てば、より安全に認証情報を入力することが可能となる。

[0077] (第3の実施形態)

第1の実施形態および第2の実施形態では、Bluetooth機器同士の間で使用する認証情報と、Bluetooth機器とBluetoothセキュリティサーバとの間で使用する認証情報とが同様であったが、第3の実施形態では、Bluetooth機器同士の間で可変な認証情報を使用し、Bluetooth機器とBluetoothセキュリティサーバ間との間で固定的な固定認証情報を使用する点異なる。第3の実施形態の構成は、第1の実施形態または第2の実施形態と同様なので詳細な説明を省略する。

[0078] 図18は、本発明の第3の実施形態のBluetoothセキュリティサーバの認証情報配布フローを示す図であり、BluetoothセキュリティサーバからBluetooth機器の認証情報を配布する手法を示す。まず、Bluetoothセキュリティサーバが、デバイス検索のためにインクワイアリ検索を使用する(ステップS2401)。応答してきたBluetooth

機器のBD__ADDRとそのデバイスクラスが、所望のBluetooth機器のものであるか確認する。該Bluetooth機器であった場合、ステップS2402へ進み、そうでなければ終了する。ステップS2602では、Bluetoothセキュリティサーバ側は、ROMに保存しているBluetooth機器との固定認証情報(第1の認証情報)を認証に使用する。ここで、上記固定認証情報は工場出荷時にメーカーが機種固有に設定した値であり、外部者には漏れていないものとする。第1の実施形態および第2の実施形態と同様に各デバイスクラス毎に固定パスキーが設定されており、Bluetoothセキュリティサーバ側は上記パスキーを認証時に使用する。Bluetooth機器側では、不揮発性メモリ404に同様の固定パスキーが工場出荷時に設定されている。

[0079] 図19は、第3の実施形態のBluetooth機器におけるBluetoothアドレスとリンクキーのリストを示す図であり、Bluetoothセキュリティサーバとの認証時に接続するための固定認証情報と、Bluetooth機器同士で接続するための可変認証情報とが設定されている。ステップS2603で、認証結果がOKだった場合はステップS2604で認証受諾しステップS2606へ、そうでない場合はステップS2605で認証拒否し終了する。ステップS2606では、BluetoothセキュリティサーバとBluetooth機器がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。サービス情報が異なった場合は終了する。ステップS2607では、BluetoothセキュリティサーバからBluetooth機器に認証情報(第2の認証情報)を配布する。この際、認証情報を配布する方法は、第1の実施形態及び第2の実施形態のどちらの方法でも構わない。Bluetooth機器は前回の可変認証情報を破棄し、配布された新しい可変認証情報を保存する。以上でBluetoothセキュリティサーバの認証情報の配布処理を終了する。

[0080] 図20は、第3の実施形態のBluetooth機器の認証情報配布フローを示す図である。最初に、BluetoothセキュリティサーバからBluetooth機器に対して認証接続を開始する。ステップS2701において、接続相手がBluetoothセキュリティサーバだった場合は、ステップS2702へ、そうでない場合はステップS2707に進む。ステップS2702において不揮発性メモリから認証情報を取得し、Bluetoothセキュリティサーバとの認証に使用する。ステップS2703では、認証結果がOKならばステップS2704に進み、認証受諾してステップS2705に進む。そうでない場合は、ステップS2710に進

み認証を拒否して終了する。

[0081] ステップS2705では、BluetoothセキュリティサーバとBluetooth機器がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。確認がOKの場合は、ステップS2706に進み、BluetoothセキュリティサーバからBluetooth機器に認証情報を配布する。そうでない場合は終了する。次にステップS2706に進み、該不揮発性メモリに取得した該認証情報を記憶し終了する。また、ステップS2707に進んだ場合、Bluetooth機器同士のBluetooth認証接続であるので、害認証時にはステップS2707で可変認証情報を認証に使用し、認証結果がOKの場合はステップS2709に進み認証を終了する。そうでない場合は、ステップS2710に進み認証拒否し終了する。

[0082] (第4の実施形態)

第1の実施形態は、認証情報を配布する対象のBluetooth機器に既存認証情報(第1の認証情報)がすでに設定されている場合のみ有効であるが、第4の実施形態は、BluetoothセキュリティサーバからBluetooth機器に認証有無の設定が行える点が異なる。第4の実施形態の機器構成は、第1の実施形態と同様なので構成についての詳細な説明は省略する。

[0083] 図21は、本発明の第4の実施形態のBluetoothセキュリティサーバの認証設定時動作フローを示す図である。ここでは、Bluetooth機器が認証無しと設定されており、BluetoothセキュリティサーバがBluetooth機器を認証有りに変更する場合について説明する。まず、ステップS2801でBluetoothセキュリティサーバが、デバイス検索のためにインクワイアリ検索を使用する。応答してきたBluetooth機器のBD_ADDRとそのデバイスクラスが所望のBluetooth機器のものであるか確認する。該Bluetooth機器であった場合、ステップS2802へ進み、そうでなければ終了する。次にステップS2802では、Bluetooth機器とBluetoothセキュリティサーバは認証無しで接続する。ステップS2803は、BluetoothセキュリティサーバとBluetooth機器がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。ステップ2804では、BluetoothセキュリティサーバからBluetooth機器に認証有りの設定を行う。

[0084] 図22は、第4の実施形態におけるBluetooth機器の認証設定の動作フローを示す

図である。まず、ステップS2901でBluetoothセキュリティサーバが、Bluetooth機器に対して認証無しで接続をしかける。次にステップS2902において、BluetoothセキュリティサーバとBluetooth機器がSDPプロトコルによりサービス情報を交換し、お互いの機能を確認する。ステップS2903では、BluetoothセキュリティサーバからBluetooth機器に認証情報を設定し、Bluetooth機器は認証有りとして設定される。

[0085] 第4の実施形態によれば、無線でBluetooth機器の接続認証の有りまたは無しを設定することが可能となる。

[0086] なお、上記のすべての実施形態の説明において、通信機器としてBluetooth規格に対応した通信機器間についての説明を行ってきたが、本発明はこれに限られるものではなく、通信部(Bluetoothセキュリティサーバ)が通信機器(Bluetooth機器)に対して、無線を介して認証情報を供給するという思想を逸脱しない範囲ですべての通信機器に対して適用が可能である。

[0087] 本発明を詳細にまた特定の実施態様を参照して説明したが、本発明の精神と範囲を逸脱することなく様々な変更や修正を加えることができることは当業者にとって明らかである。

本出願は、2004年3月2日出願の日本特許出願(特願2004-57393)に基づくものであり、その内容はここに参照として取り込まれる。

産業上の利用可能性

[0088] 本発明の通信システムおよび通信方法によれば、通信機器に対して、無線を介して前記認証情報を供給することにより、通信機器は、従来の無線通信機能を利用して認証情報を取得でき新たに認証情報の入力手段を設ける必要がない為、通信システムのコストを削減できる効果を有し、認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信システムおよびその通信方法等に有用である。

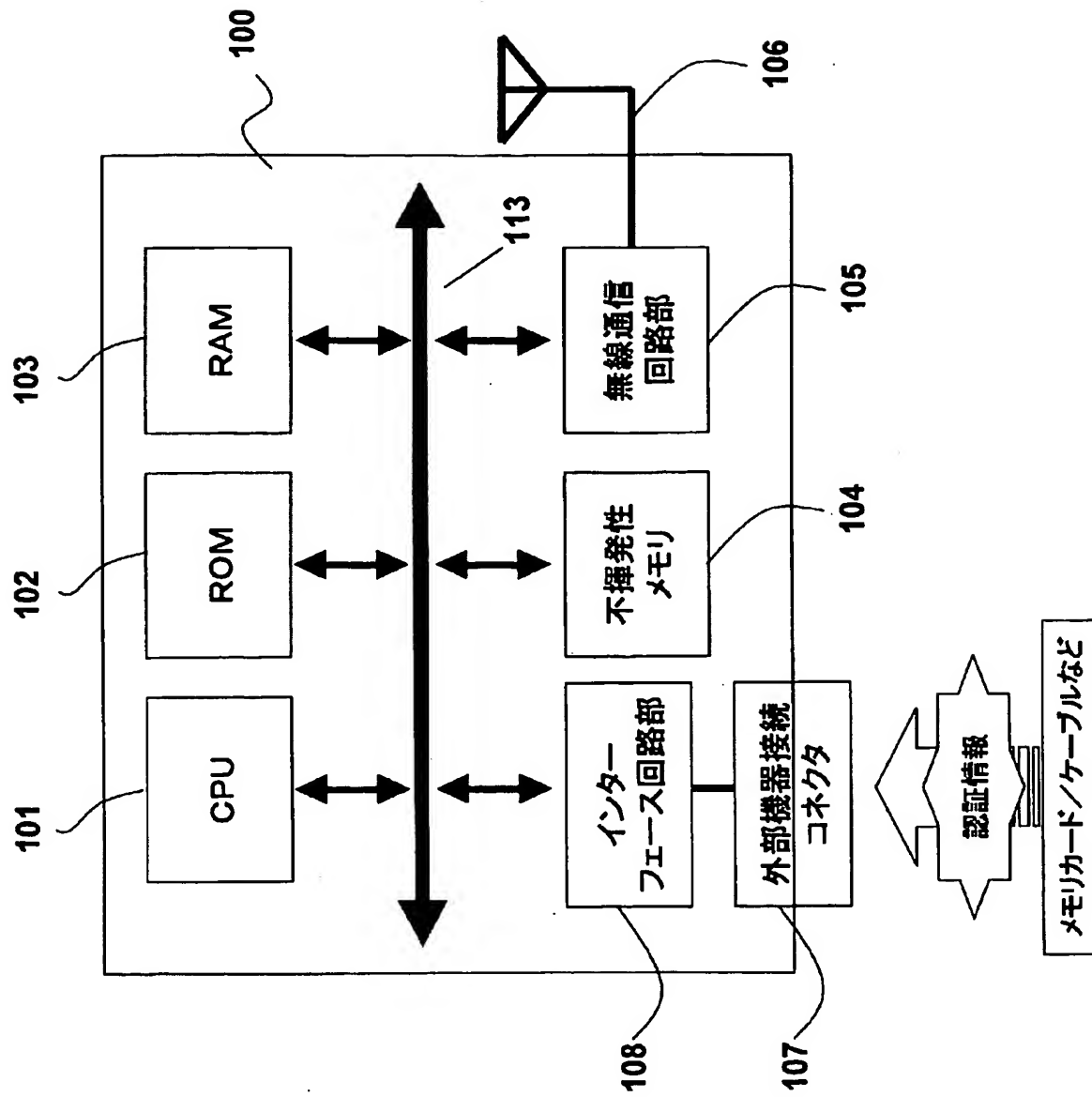
請求の範囲

- [1] 認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信システムであって、
前記少なくとも2台のうち少なくとも1台の通信機器に対して、無線を介して前記認証情報を供給する通信部を備える通信システム。
- [2] 前記通信部は、前記少なくとも2台の通信機器のうち特定の通信機器に備えられていることを特徴とする請求項1に記載の通信システム。
- [3] 前記特定の通信機器に備えられた前記通信部は、前記少なくとも2台の通信機器のうち前記特定の通信機器以外の通信機器に対して、前記認証情報を供給することを特徴とする請求項2に記載の通信システム。
- [4] 前記通信部は、前記少なくとも2台の通信機器と独立に備えられていることを特徴とする請求項1に記載の通信システム。
- [5] 前記通信部は、外部インタフェースを備え、前記外部インタフェース経由で前記認証情報を受け取することを特徴とする請求項1に記載の通信システム。
- [6] 前記通信部は、前記外部インタフェースに接続されたメモリカードに保存された前記認証情報を前記外部インタフェース経由で受け取することを特徴とする請求項5に記載の通信システム。
- [7] 前記少なくとも1台の通信機器は、各通信機器に予め定められた固有の第1の認証情報を用いて前記通信部と認証を行う機能と、前記第1の認証情報とは異なる第2の認証情報を用いて前記少なくとも2台の通信機器間の認証を行う機能とを備えることを特徴とする請求項1に記載の通信システム。
- [8] 前記認証情報は、予め各通信機器に定められ前記通信部と前記少なくとも1台の通信機器との間で用いられる各機器固有の固定認証情報と、任意に生成され前記少なくとも2台の通信機器間の通信に用いられる可変認証情報とを含むことを特徴とする請求項1に記載の通信システム。
- [9] 前記認証情報は、通信相手のアドレス情報またはパスワード情報であることを特徴とする請求項1に記載の通信システム。
- [10] 前記少なくとも2台の通信機器間の通信または前記少なくとも1台の通信機器と前

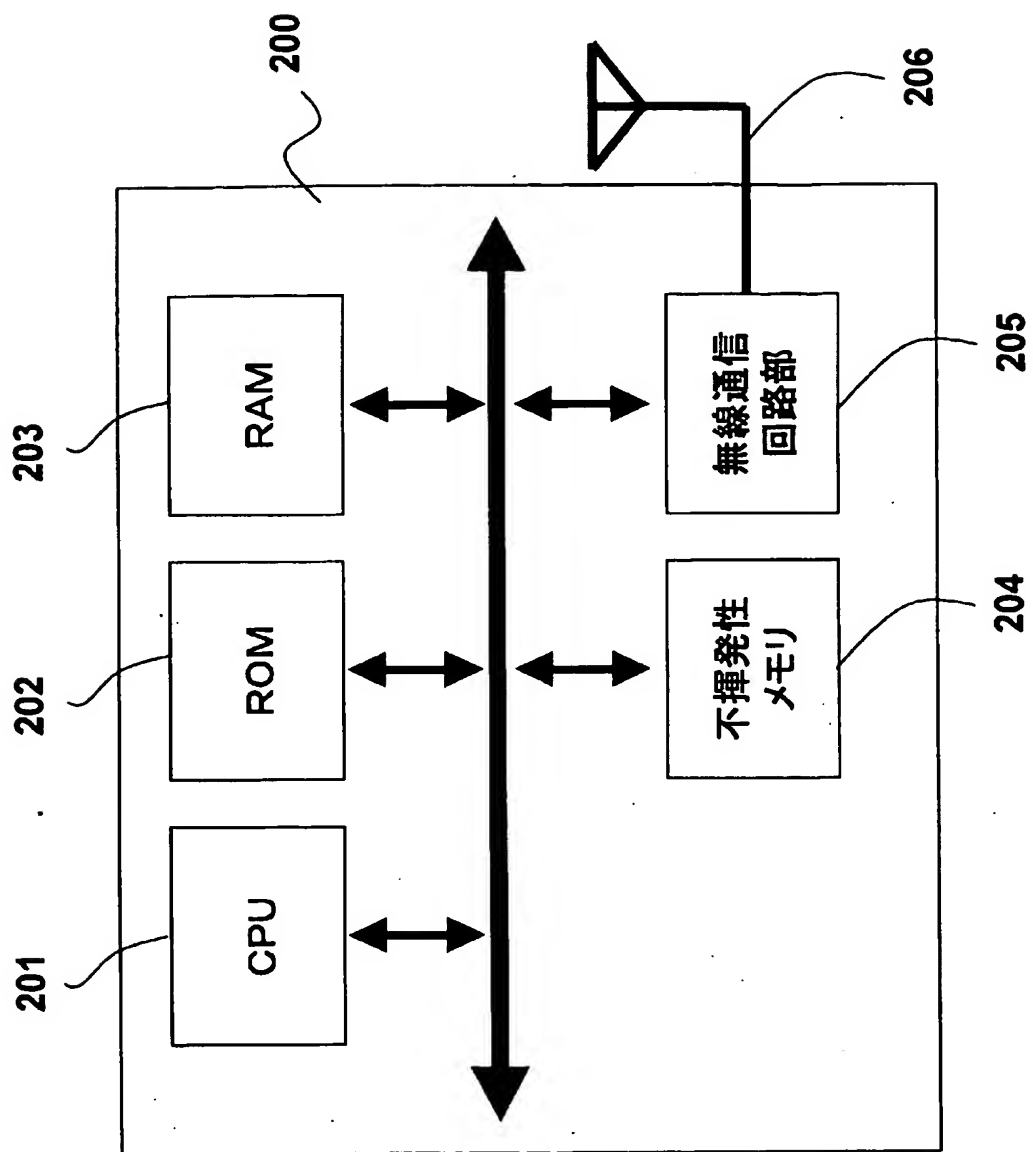
記通信部との間の通信が、Bluetooth規格の無線通信であることを特徴とする請求項1〜9のいずれか1項に記載の通信システム。

- [11] 認証情報を用いた認証機能を有し、少なくとも2台の通信機器間において互いに通信可能な通信方法であって、
前記少なくとも2台の通信機器のうち少なくとも1台の通信機器に対して、無線を介して前記認証情報を供給する供給ステップを有する通信方法。
- [12] 前記供給ステップは、前記少なくとも2台の通信機器のうち特定の通信機器と前記少なくとも2台の通信機器のうち前記特定の通信機器以外の通信機器間で実行されることを特徴とする請求項11に記載の通信方法。
- [13] 前記少なくとも1台の通信機器に対して、前記少なくとも1台の通信機器に予め定められた固有の第1の認証情報を用いて認証を行なう第1の認証ステップをさらに有し、
前記第1の認証ステップで認証された場合に、前記認証情報は前記少なくとも1台の通信機器に供給されることを特徴とする請求項11に記載の通信方法。
- [14] 前記少なくとも1台の通信機器が受け取る前記第1の認証情報とは異なる第2の認証情報を用いて前記少なくとも2台の通信機器間の認証を行なう第2の認証ステップをさらに有する請求項13に記載の通信方法。
- [15] 前記少なくとも2台の通信機器間の通信または前記少なくとも1台の通信機器への通信が、Bluetooth規格の無線通信であることを特徴とする請求項11〜14のいずれか1項に記載の通信方法。
- [16] 認証情報を用いて互いに通信可能であるか認証する機能を有し認証後に通信を開始する通信機器であって、
前記認証情報を無線を介して取得する手段を備える通信機器。

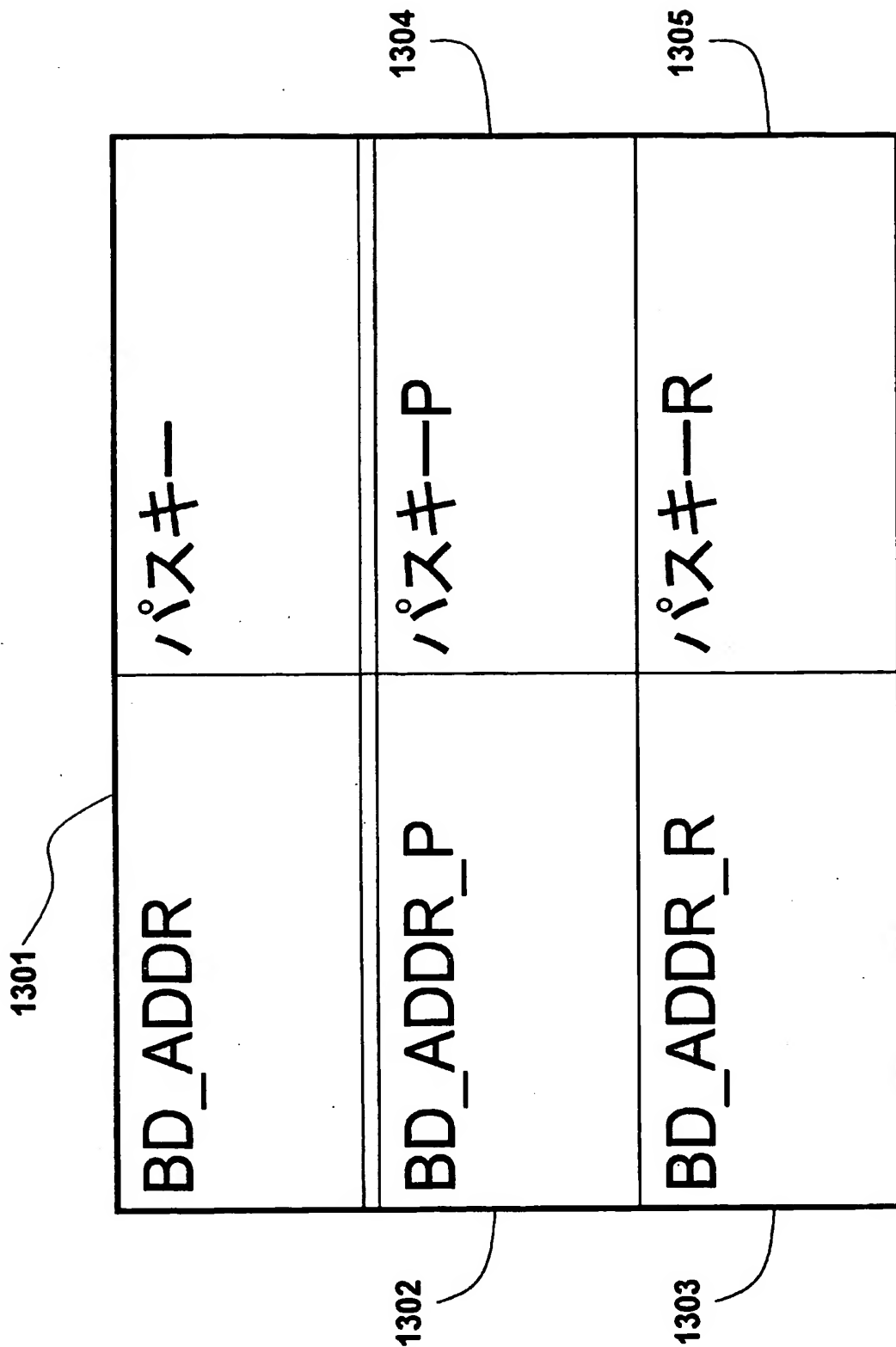
[図1]



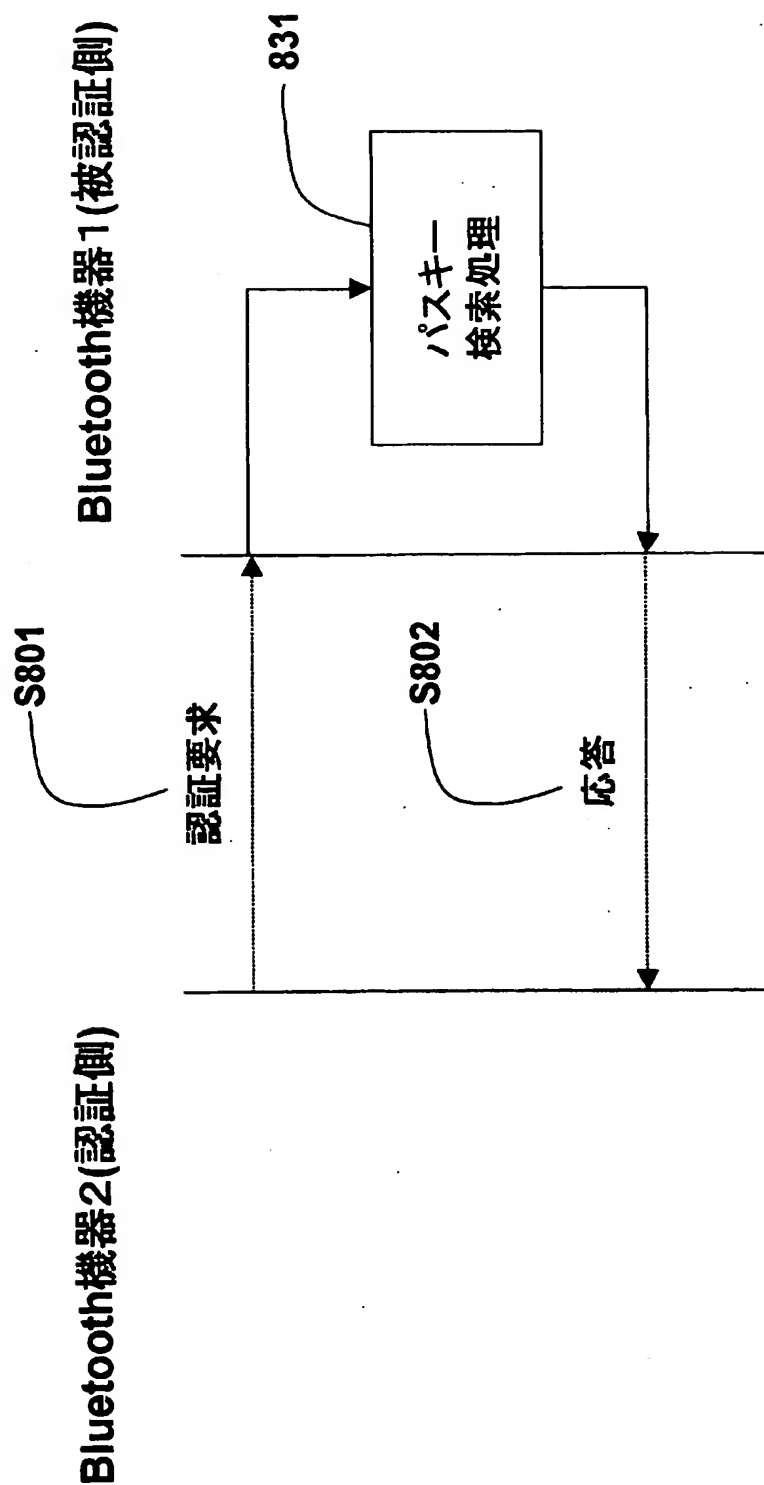
[図2]



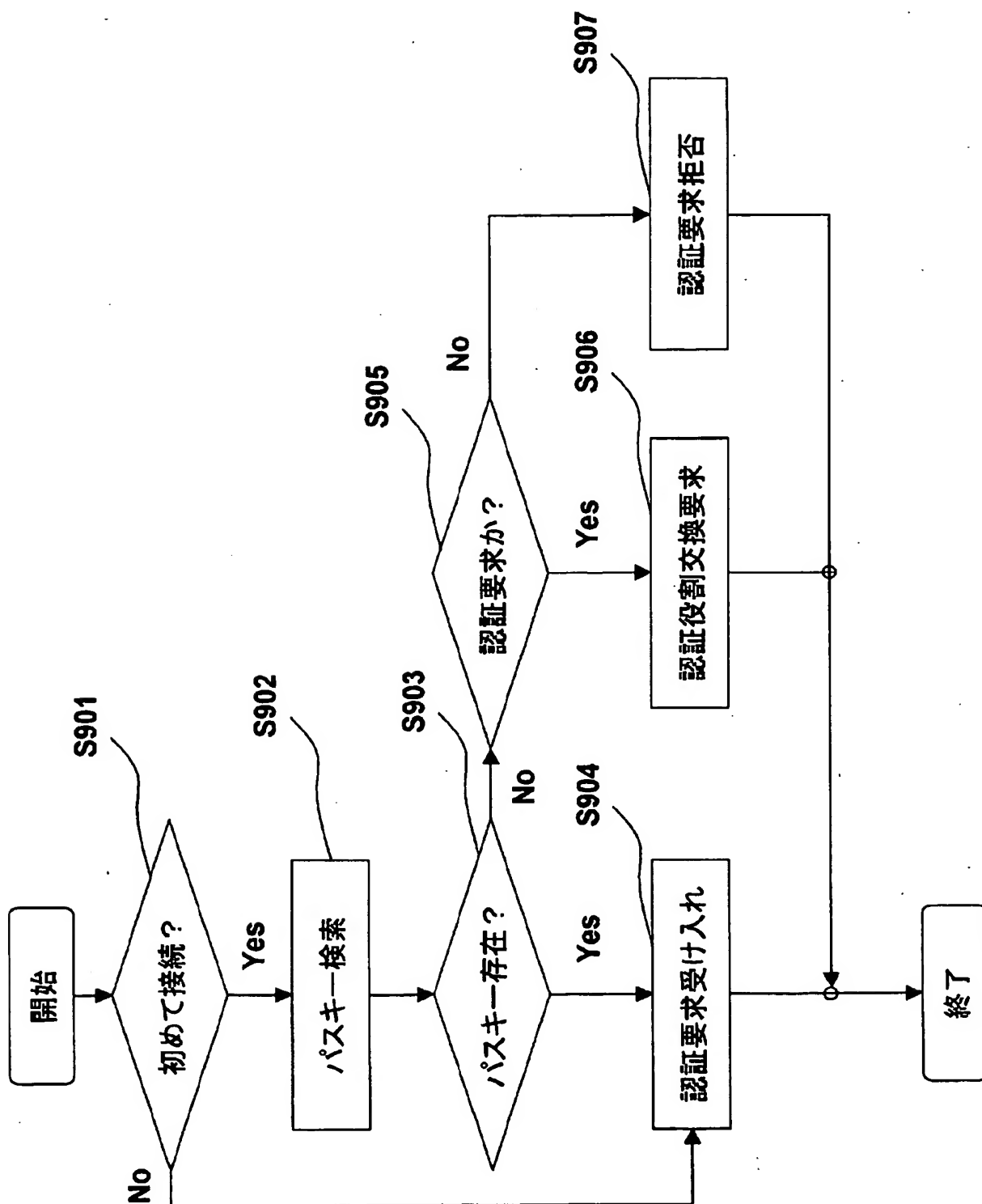
[図3]



[図4]



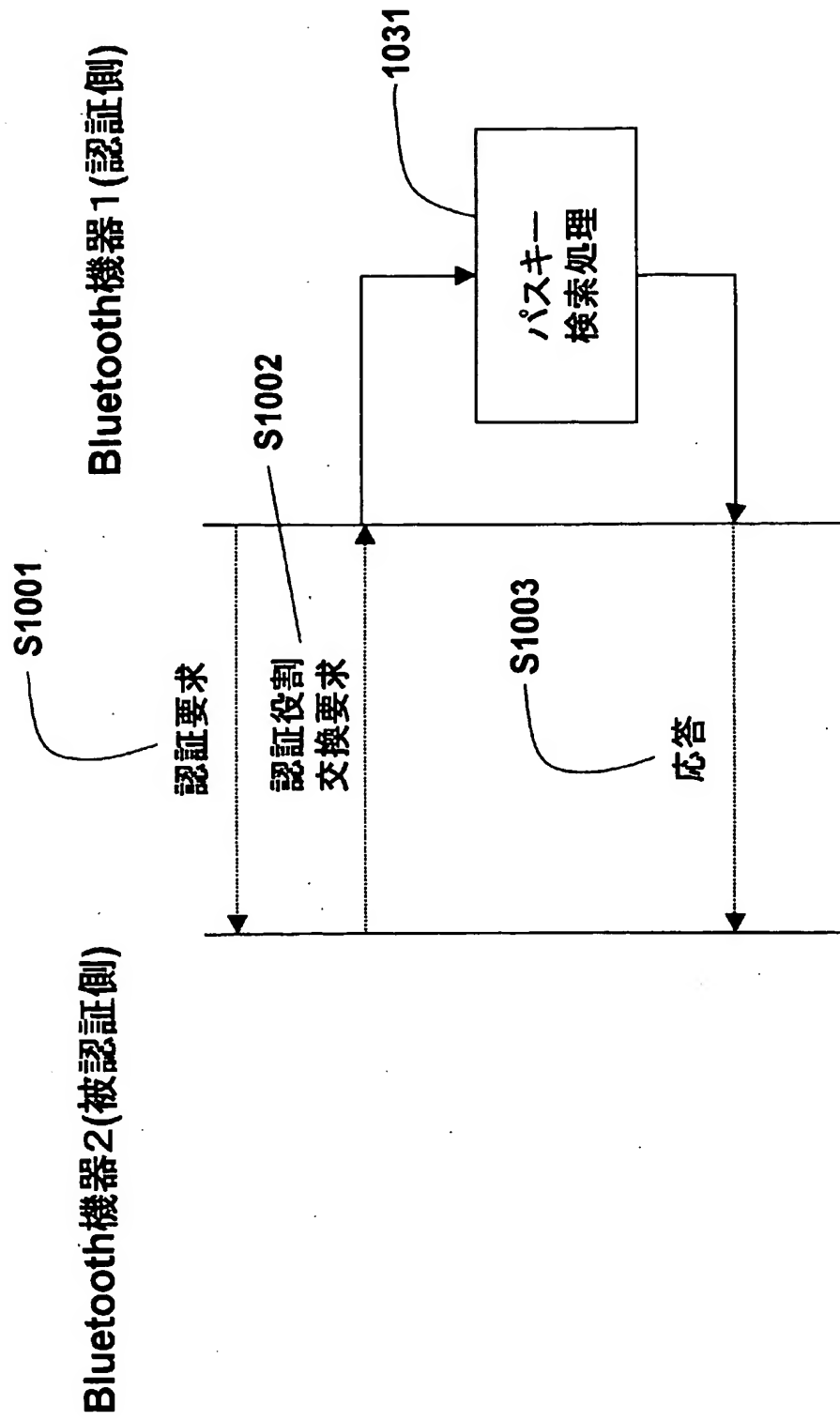
[図5]



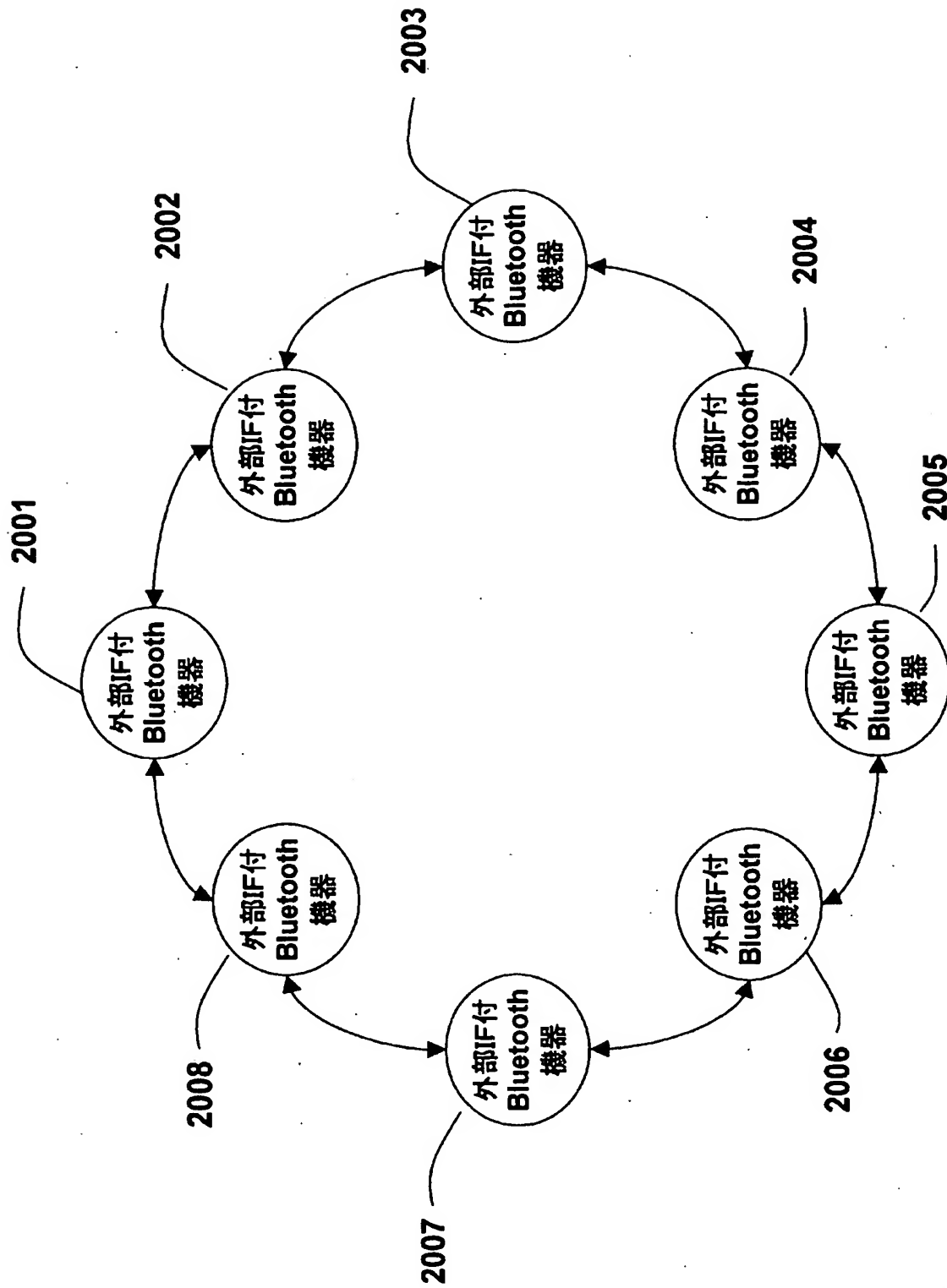
[図6]

BD_ADDR	LINK_KEY	1101
BD_ADDR_A	KEY_A	
BD_ADDR_F	KEY_F	
BD_ADDR_Z	KEY_Z	
1102	1103	
1104	1105	
1106	1107	

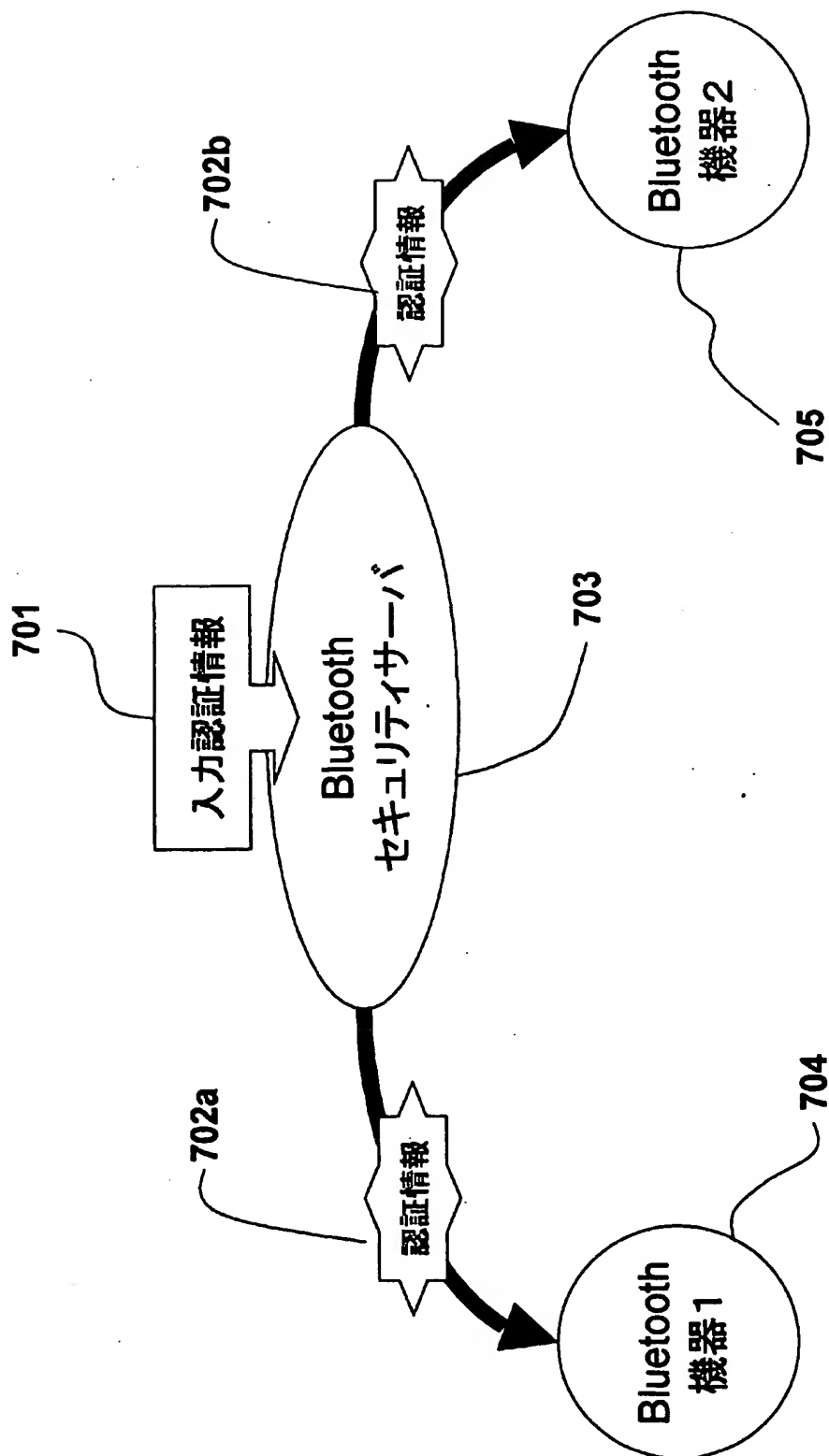
[図7]



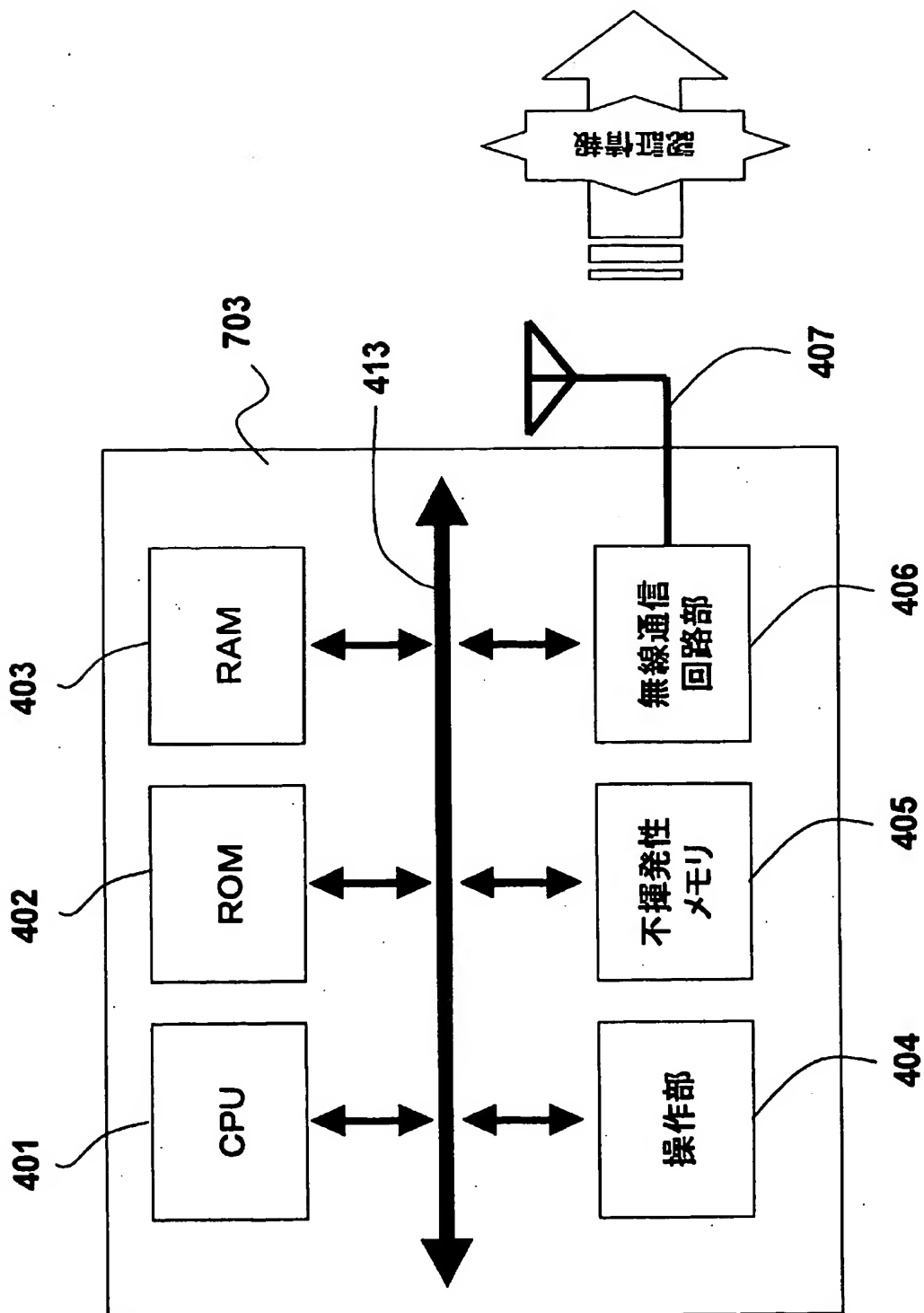
[図8]



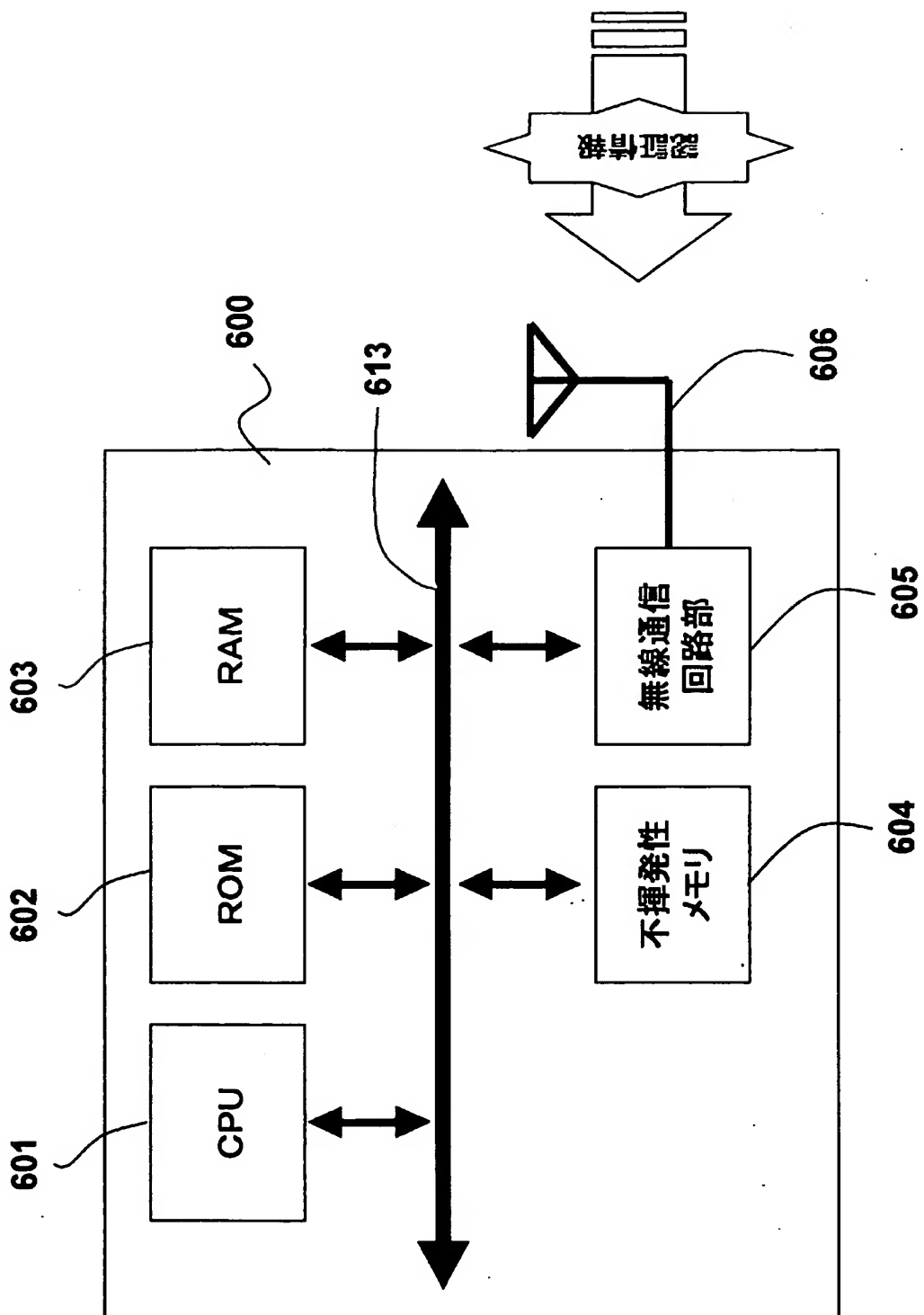
[図9]



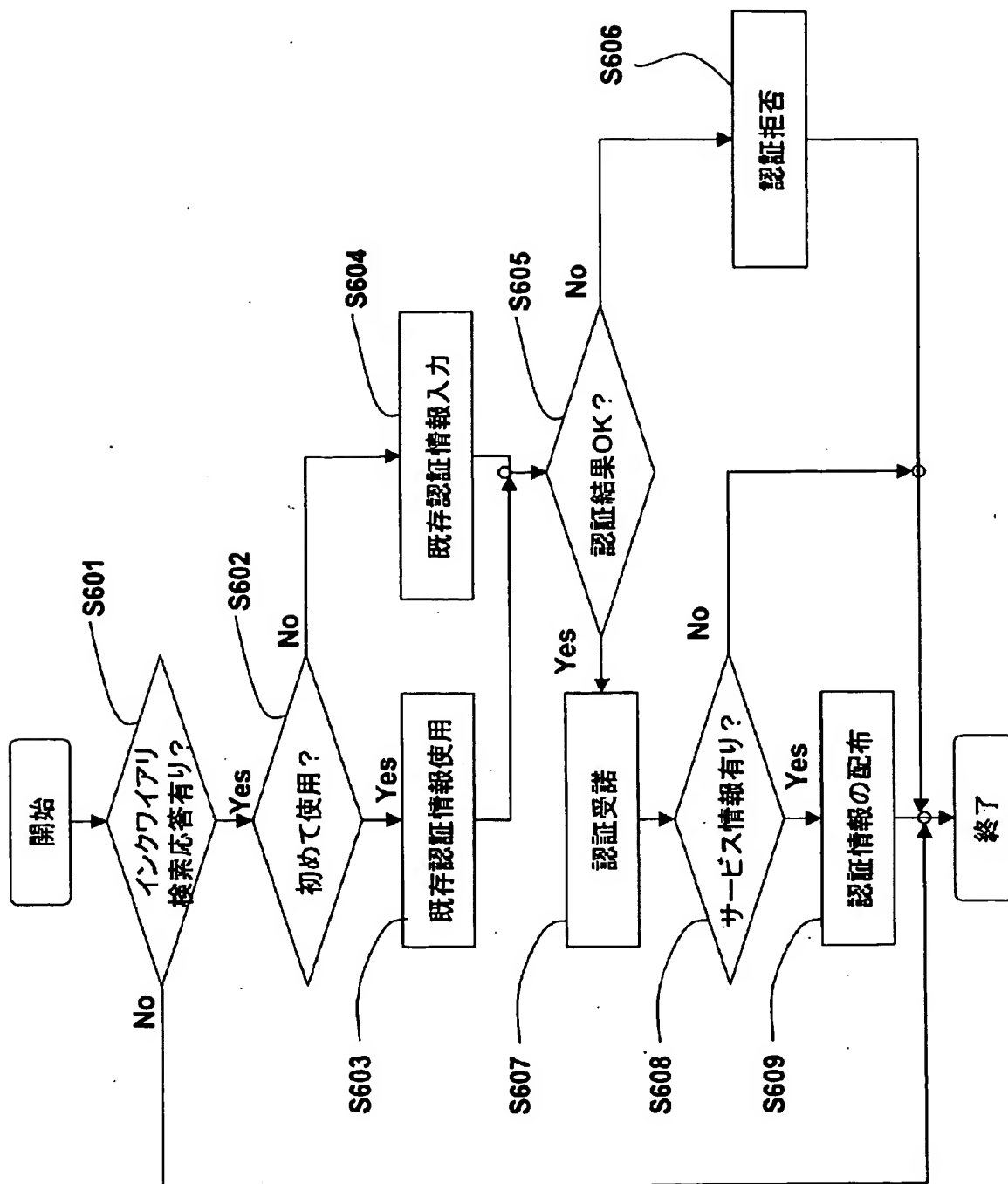
[図10]



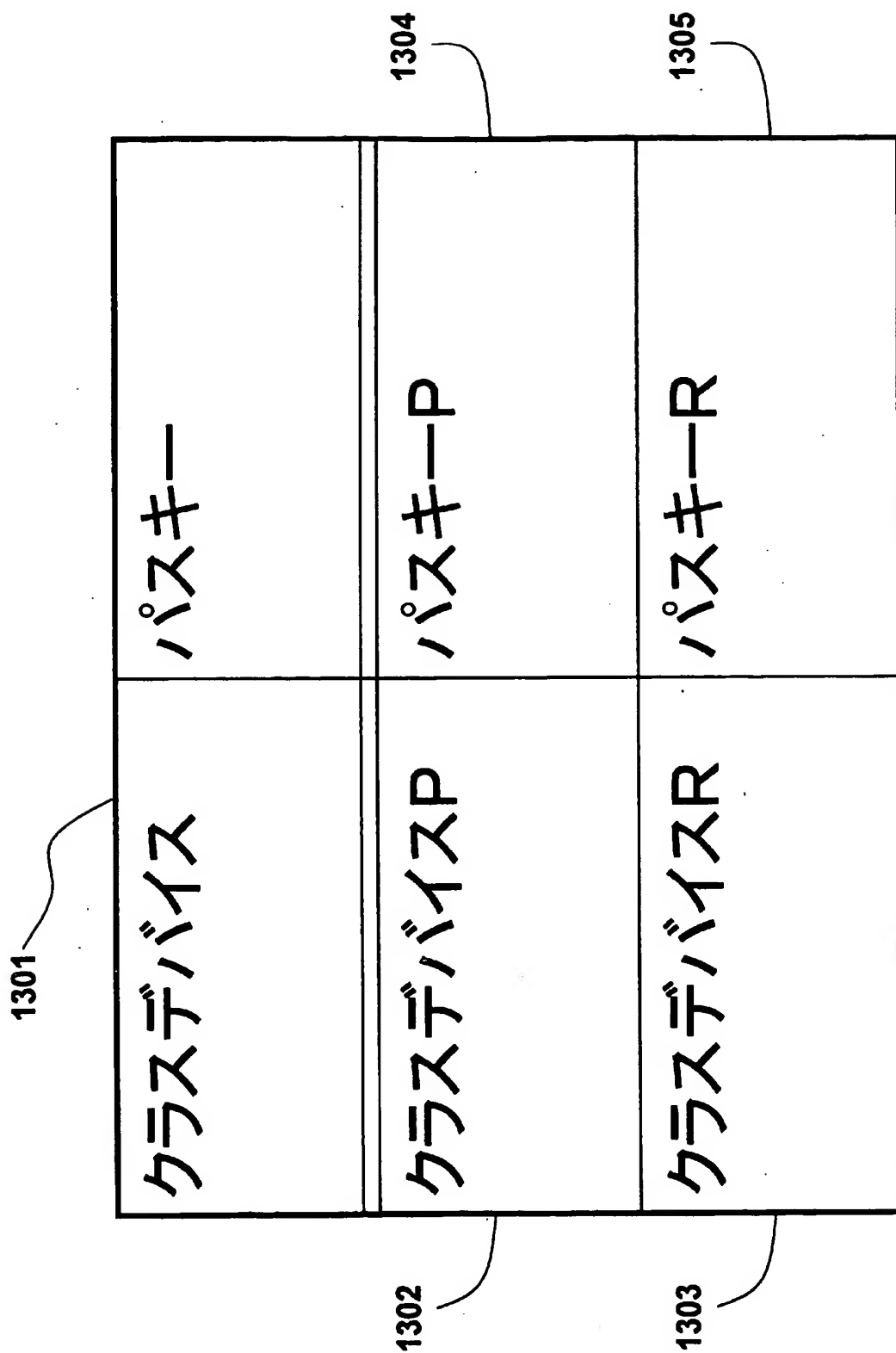
[図11]



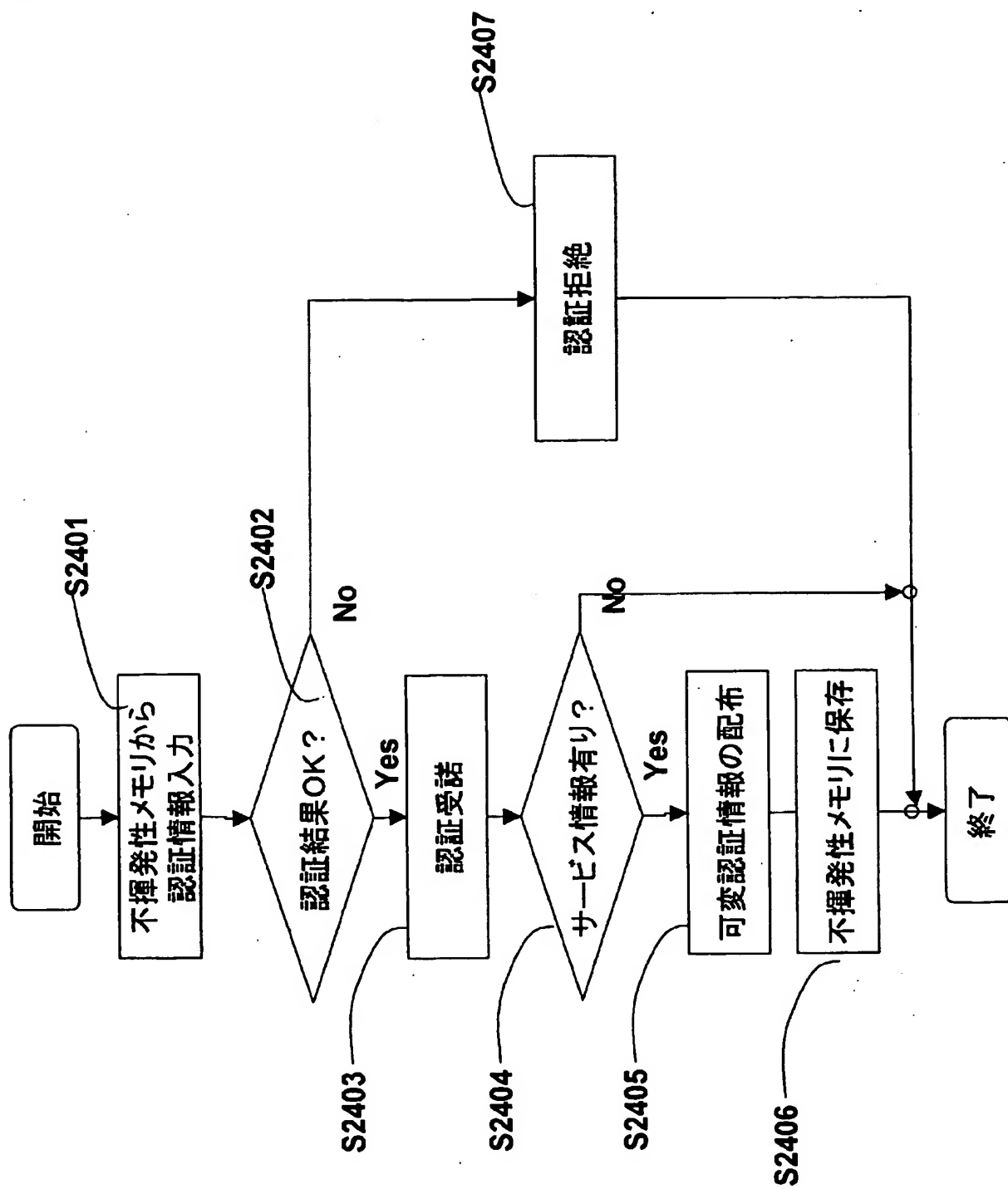
[図12]



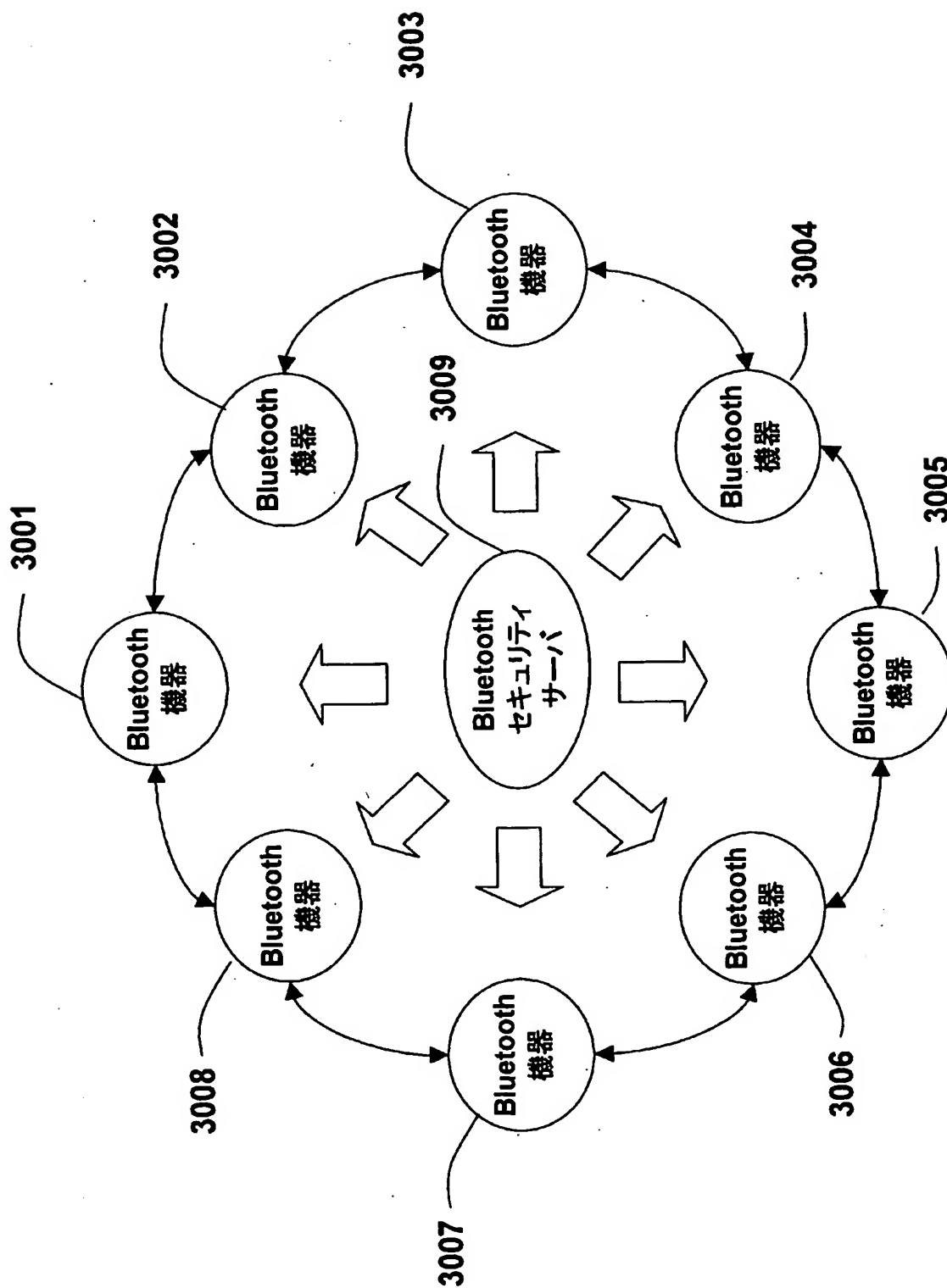
[図13]



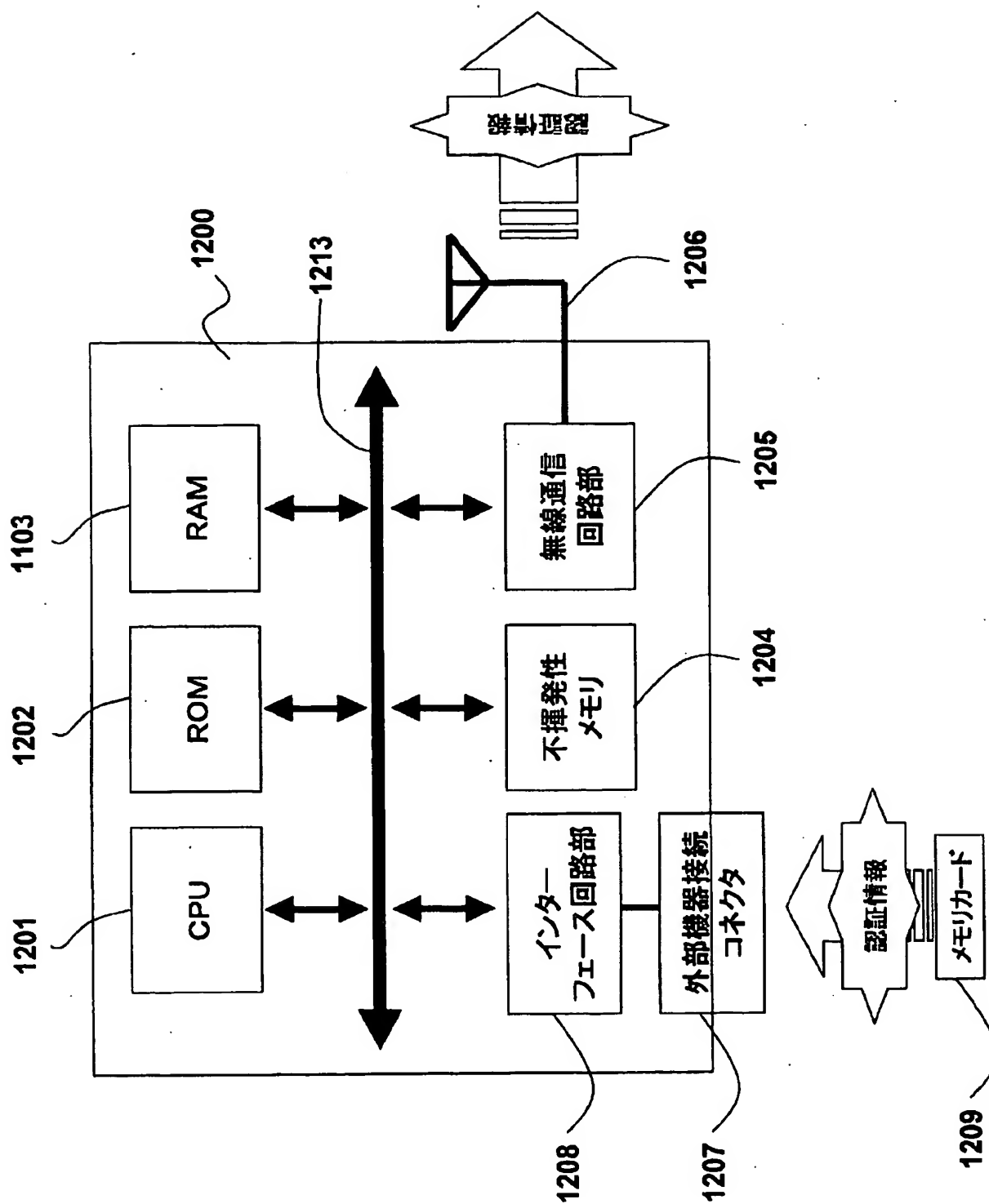
[図14]



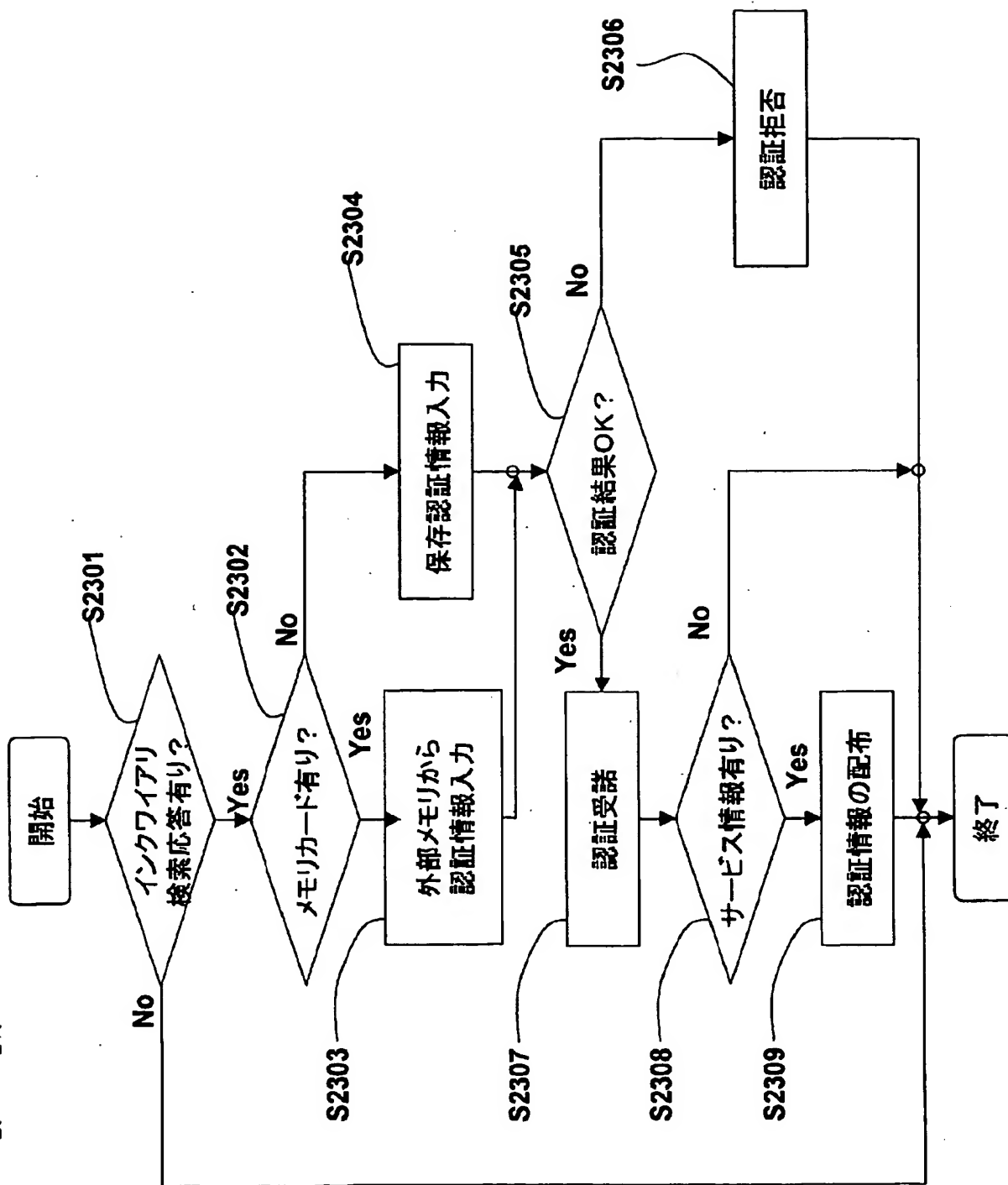
[図15]



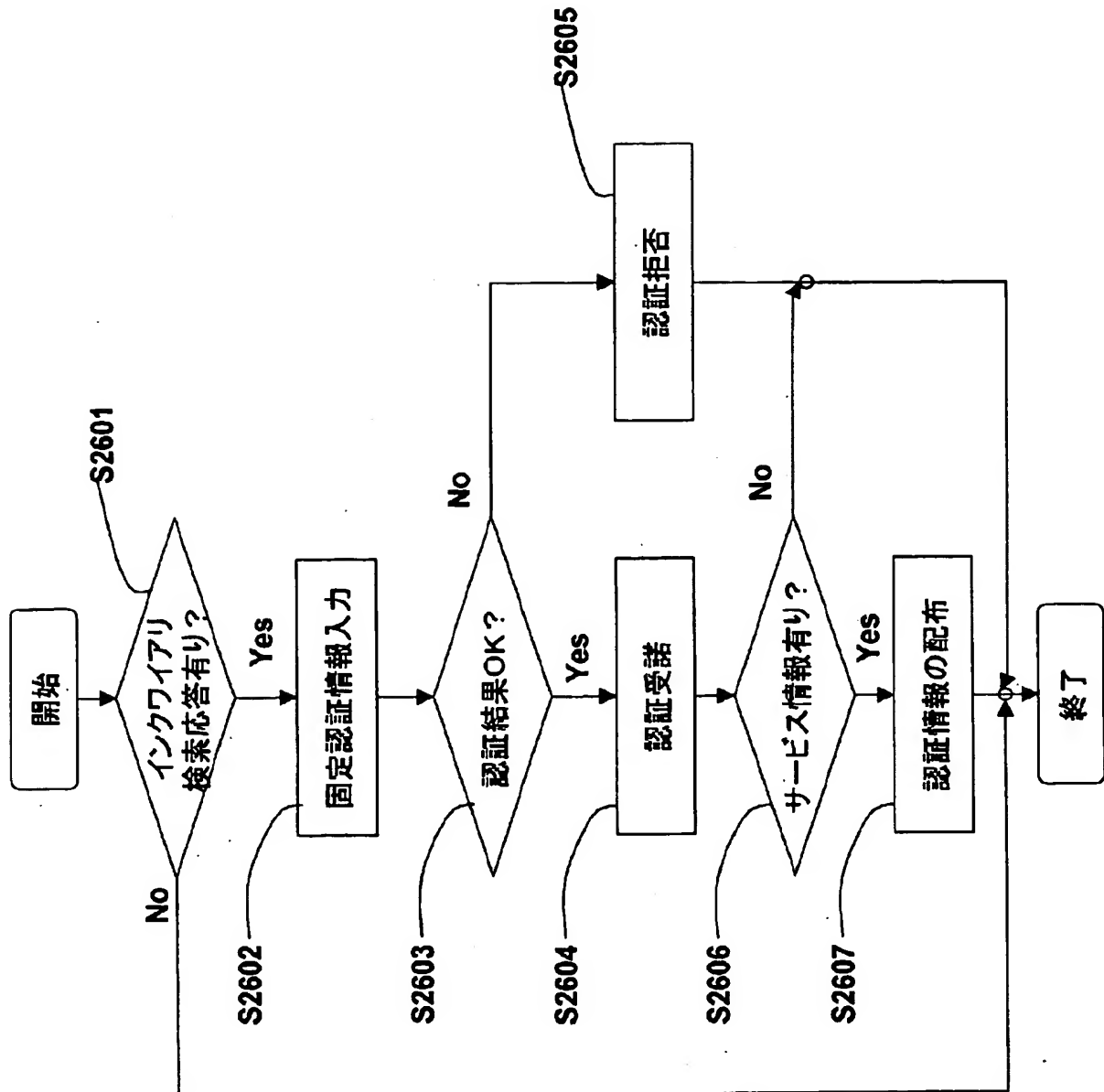
[図16]



[図17]



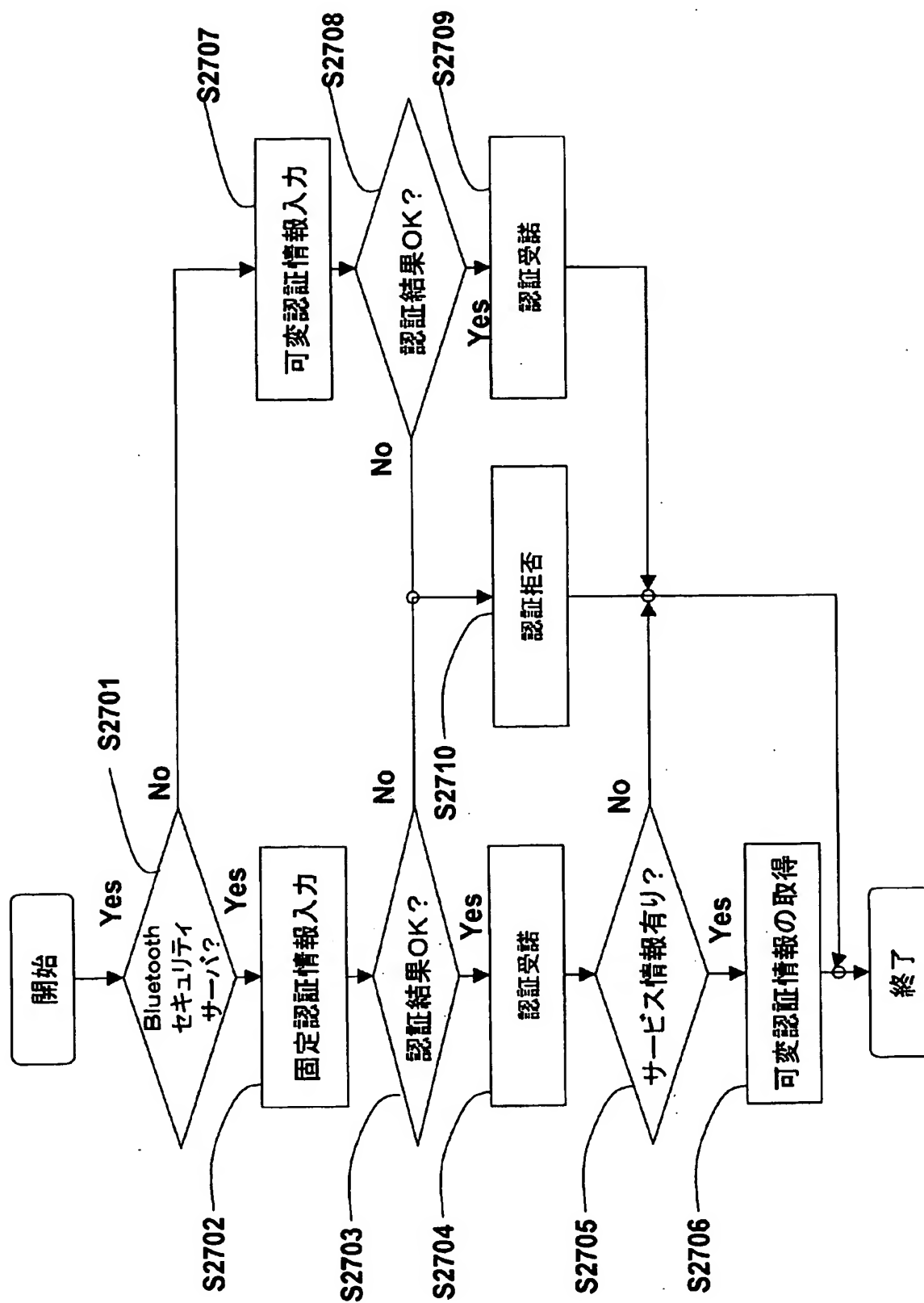
[図18]



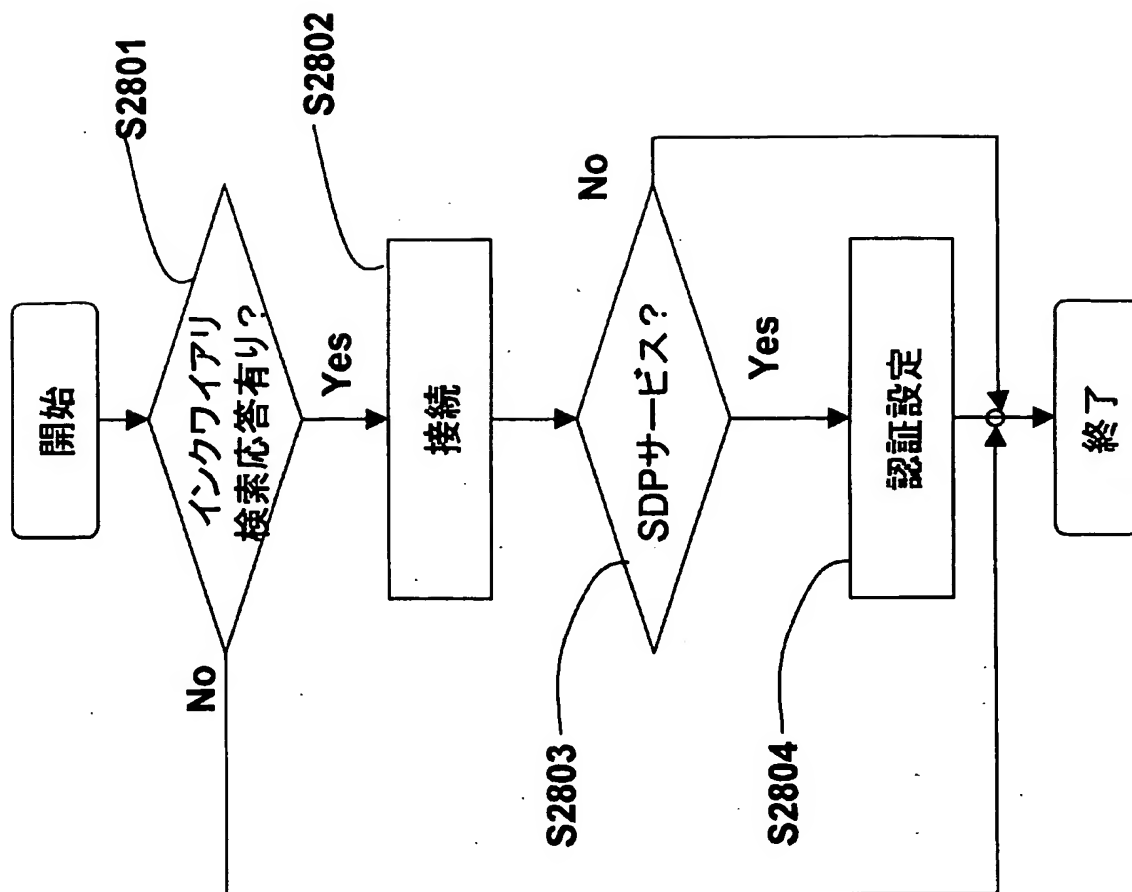
[図19]

BD_ADDR	パスキー	2501	2502
BD_ADDR_F	固定パスキーF		
BD_ADDR_K	可変パスキーK		
		2503	2504
		2505	

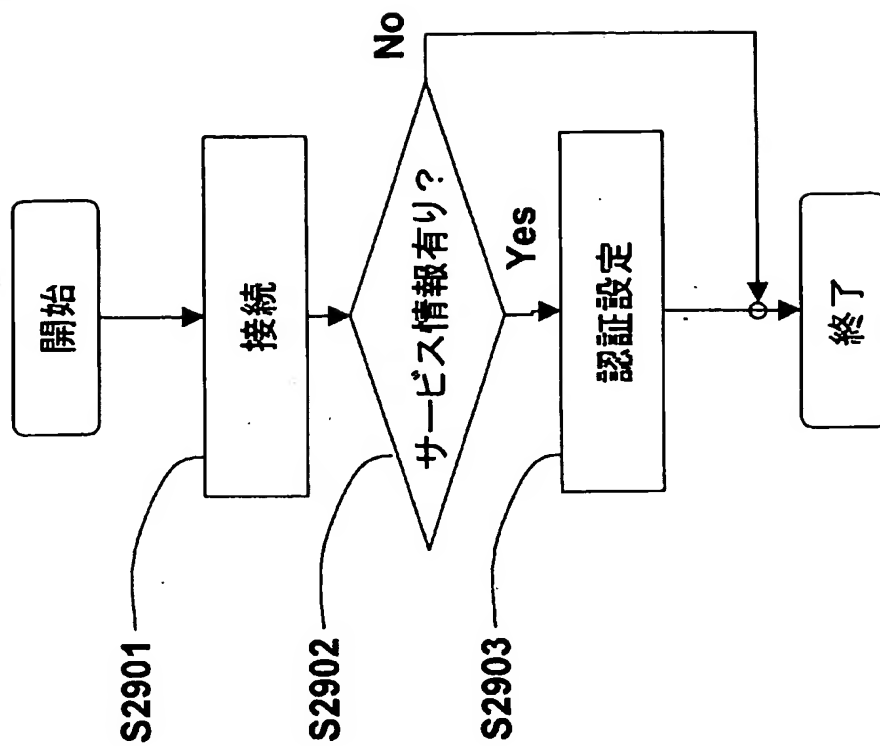
[図20]



[図21]



[図22]



[図23]

